BY ORDER OF THE
SECRETARY OF THE AIR FORCE

AIR FORCE INSTRUCTION 31-101, VOLUME 1
1 DECEMBER 1996

Security

★*THE AIR FORCE PHYSICAL SECURITY PROGRAM*

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

This instruction implements Air Force Policy Directive (AFPD) 31-1, *Physical Security.* It provides guidelines, procedures, and details of minimum security levels that the Air Force (AF) requires to maintain, project, and execute air power. AFI 31-101 Volume 2 *The Air Force Nuclear Security Program Standards* is designed for use by units supporting nuclear resources and supplements the guidance provided in this instruction. This instruction applies to all Department of the Air Force civilian personnel. The terms "must," "shall," and "will" denote mandatory actions in this instruction. Any organization may supplement this instruction. Major command (MAJCOM) and direct reporting units send one copy of supplements to HQ AFSPA/SPS, 8601 F. Ave SE, Kirtland AF Base (AFB), NM 87117-5664.

CORRECTED COPY -- THIS REPUBLISHING IS INTENDED PRIMARILY TO PROVIDE ADMIISTRATIVE CHANGES TO THE 1 DECEMBER 1996 VERSION OF THIS AFI.

SUMMARY OF REVISIONS

This revision corrects administrative errors, updates references where required, and incorporates minor clarifications and changes from the MAJCOMs and field units. Chapter 1 includes alternatives for fences at free zone boundaries surrounding nuclear areas; allows security priority downgrading of aircraft undergoing depot level maintenance at the operational location; adds sections concerning "economy of force" and "TPC material"; and adds a requirement for a brief description of incidents where aerospace resources are damaged. Chapter 3 modifies the definition of a Helping Hand and establishes reporting for security police lessons learned. Chapter 4, specifies that the MAJCOM determines the approval authority of deviations for nonnuclear security standards. Chapter 5, changes coordinating official to approving official; removes the restriction on coding restricted area badges (RABs); changes procedures for recording destruction of RABs; clarified the term "visitors" and clarifies visitor procedures for areas supported by AECS; defines designated vouching authority; incorporates the use of an AF Form 1109, *Visitor Register Log* at nuclear areas; incorporates clarification on FCDNA inspectors hand-carrying their EAL and presenting it upon arrival at the inspected unit; incorporates signature verification procedures for AF Form 2586. Chapter 6 specifies only one AFT must remain in the AFT facility; clarifies the requirement when splitting an ART into one-person mobile patrols; adds the term Fighting Load (FL) and the Basic Quantity (BQ) and specifies the issue of the FL when supporting nuclear resources; adds a new paragraph on equipment including body armor selection. Chapter 7 clarifies CSC direct line communications between security posts; clarifies fence and vegetation specifications for nonnuclear areas; clarifies boundary lighting standards and test criteria for nuclear areas; added exceptions for Barksdale and Nellis AFBs concerning area lighting requirements; clarifies lighting check requirements; addresses facility spacing in relation to the base perimeter; corrects diameter of fencing wire requirement; and clarifies AFT garage door hardening requirements. Chapter 8 specifies MAJCOMS plan P3I replacement programs to support IDS; addresses computer based event priority of annunciation; addresses testing issues; includes the two-person BISS maintenance concept; clarifies certification and tamper testing for nuclear IDS; requires SEI 323 qualified personnel as MSCFOs; and revises compensatory measures for alarm system failures. Chapter 9 requires alternate power facilities to be locked or alarmed and allows use of DoD guards as off-base response force members. Chapter 10 clarifies numerous space systems requirements including adding figures 10.1 through 10.5 to display

Supersedes: AFI 31-101, Volume 1, 10 November 1994. Certified by: HQ USAF/SP (Colonel Andrew A. Corso)
OPR: HQ AFSPA/SPSS (CMSgt Jack P. Laws) Pages: 69/Distribution: F

security priorities of space systems and consolidating security requirements into a new paragraph 10.10. Chapter 11 revises WS3 URC storage and clarifies Type I and II arrival and departure procedures. Chapter 12 revises security force requirements for C2 aircraft. Chapter 13 and 14, update aircraft terminology. Chapter 15, figure 15.1. clarifies security priorities, and clarifies security requirements for presidential, SENEX, SDSAM, and SAM aircraft. In chapter 16, figure 16.1. clarifies security priority and requirements for SCI facilities.

Paragraph

Paragraph

Paragraph

Paragraph

Paragraph

Page

Figures

Attachments

PART 1
PROGRAM CONCEPTS AND ADMINISTRATION

Chapter 1

PROGRAM CONCEPTS AND COMPLIANCE

1.1. Concept of the AF Physical Security Program. Implement this program by designing a security program that deters and responds to hostile operations against priority resources. It is critically important that intelligence gathering and analysis continue throughout the life of the security program. You can achieve the appropriate degree of deterrence and have an effective physical security program by designing a security system that detects hostile activity, controls entry and access to sensitive areas, and if necessary, defeats a hostile force. Units supporting nuclear weapons must use this instruction in conjunction with AFI 31-101, Vol II, to achieve complete understanding of AF nuclear security concepts and policy.

1.1.1. Security Threat Analysis. Working with intelligence agencies, particularly Air Force Intelligence (IN) and the Air Force Office of Special Investigations (AFOSI), MAJCOMs must analyze potential threats. Use this analysis along with *INKT 2660-01, Air Base Systems (ABS) Threat Support Document, Threat Compendium Worldwide Threat to Air Bases*, to plan security operations and secure nonnuclear weapons systems. Use the postulated threat in DoD C-5210.41-M, *Nuclear Weapons Security Manual*for nuclear weapon systems.

1.1.2. During wartime and transition to war, you must seek out the best ground threat intelligence available to determine what measures beyond peacetime actions you should take to protect air force resources. In overseas areas, the Air Force Base Defense program should be used. In CONUS, most aerospace resource assumes a more active and important national security role and the physical security provided should be consistent with command war plans.

1.2. Security Priority System. This system identifies critical Air Force resources you must secure and indicates the amount of security effort you should dedicate to those particular resources. The Security Priority System recognizes owners and users of such resources must accept a varying degree of risk. The operating commands of such resources must propose a security priority for a specific resource based on the parameters specified in the following paragraphs. Where commanders do not fiscally support a resource at the currently assigned security priority level, they must ask to change the security priority and document the acceptance of greater physical security risk from the Air Force threat.

1.3. Security Priority A Resources. Assign this top-level security priority to any resource of the United States Air Force (USAF) for which loss, destruction, misuse, or compromise would gravely harm the strategic capability of the United States (US) or when the resources are politically and militarily critical to the US. In judging whether to designate a resource as priority A, consider the possible impact damage to or destruction of a specific resource would have on our national defense at home and abroad, our status as a world power, our ability to deter hostilities and/or our ability to successfully execute contingency plans and conduct warfare.

1.3.1. Examples of Security Priority A Resources:

1.3.1.1. Nuclear weapons.

1.3.1.2. Command, Control, Communications, and Computers (C4) systems critical to the success of active nuclear missions.

1.3.1.3. Critical space and launch resources.

1.3.1.4. Aircraft designated to transport the President of the United States.

1.3.2. Securing Priority A Resources. The Air Force accepts very little risk with these resources. The security forces and equipment supporting security priority A resources provide the best capability to deter, detect, and successfully engage the threat (or, where applicable, the DoD postulated threat to nuclear weapons). Secure security priority A resources by:

1.3.2.1. controlling entry to the area and the individual resource.

1.3.2.2. Expanding the security area of interest through the use of a successive series of security screens and active patrolling to reduce the standoff threat.

1.3.2.3. Providing continuous intrusion detection and surveillance at the boundary and resource. Use posted sentries when IDS is not installed or operational.

1.3.2.4. Providing dedicated response forces (RFs) inside and outside the restricted area.

1.4. Security Priority B Resources. Assign security priority B to any USAF resource for which loss, theft, destruction, misuse, or compromise would likely cause great harm to the warfighting capability of the US.

1.4.1. Examples of Security Priority B Resources:

1.4.1.1. Nonnuclear alert forces.

1.4.1.2. Expensive systems, limited in number, or one of a kind, such as:
1.4.1.2.1. Command, control, and communications (C3) facilities, systems, or equipment.
1.4.1.2.2. Vital computer facilities and equipment.
1.4.1.2.3. Designated space and launch systems.
1.4.1.2.4. Intelligence gathering systems.
1.4.2. Securing Security Priority B Resources. The Air Force accepts some internal and external risk associated with these resources. The security forces and equipment supporting security B resources must deter, detect, and successfully engage the threat. The risk associated with persons legitimately working within the restricted area is greater and the number of response forces to repel the threat is normally smaller than those provided for security priority A. The standoff risk is also greater since fewer resources are available to project the security area of interest. Secure priority B resources by:
1.4.2.1. Controlling entry to the restricted area.
1.4.2.2. Providing continuous intrusion detection and surveillance at the boundary and resource. Post sentries when IDS is not installed or operational.
1.4.2.3. Maintaining dedicated RFs inside and outside the restricted area.
1.4.2.4. Intelligence-gathering systems.

1.5. Security Priority C Resources. Assign security priority C to any USAF resource for which loss, theft, destruction, misuse, or compromise would damage US warfighting capability or could compromise the defense infrastructure.
1.5.1. Examples of Security Priority C Resources:
1.5.1.1. Weapons systems not on alert but programmed for alert status.
1.5.1.2. Selected C3 facilities, systems, and equipment.
1.5.1.3. Non-launch-critical or non-unique space launch systems (SLSs) and equipment.
1.5.1.4. Intelligence-gathering systems not critical to US operational capability.
1.5.2. Securing Priority C Resources. The Air Force accepts greater internal and external risk associated with these resources. The security forces and equipment supporting priority C resources must deter, have some capability to detect, and have the capability to engage the threat until additional forces arrive. The risk associated with persons legitimately working within the restricted area is greater and the potential for covert entry into the area is increased. The number of response forces to repel the threat is smaller than those provided for security priority B. The standoff attack risk is approximately the same as for priority B resources. Secure priority C resources by placing support and security forces in the restricted area, reinforcing them with external RFs and providing boundary detection and surveillance.

1.6. Identifying Priorities for Specific Systems. The security priorities for specific critical resources are discussed in Chapters 9 through 16. If you find the requirements of the systems security standards in Chapters 9 through 16 conflict with the requirements found in Chapters 1 through 8, follow the system security standard. Use the installation security regulation to identify the security priority of resources on an installation or on a dispersed site supported by an installation.
1.6.1. Don't assign operational taxiways and runways a security priority (see para 1.7 below).
1.6.2. Don't assign peacetime alert crews or billets a security priority (see para 1.7 below).
1.6.3. Aircraft removed from their restricted areas for maintenance retain a security priority. Establish local procedures to ensure that security forces know where to find the aircraft undergoing maintenance. See also Paragraph 1.8.
1.6.4. Owning and using personnel must secure maintenance hangars and notify security forces when aircraft are unattended.
1.6.5. Don't assign a security priority based the presence of classified information, installed classified equipment or classified material carried as cargo.
1.6.6. Protect classified material and components according to guidance in Department of Defense (DoD) 5200.1-R, *Information Security Program Regulation,* Jun 86,and AFI 31-401, *Information Security Program Regulation.*

1.7. Establishing Security Priorities. Assigned security priorities provide the basis for programming security manpower and equipment. Certain systems, such as nuclear weapons and presidential support aircraft are always security priority A at the direction of authorities above the Air Force. The Air Force determines the security priority of the other systems it operates after the operating commands recommend and coordinate, when appropriate, with the staffs of supported CINCs. Security priority levels of various resources can change during periods of increased military tension. As systems reach an increased state of readiness, their relative political and military importance increases, and commanders may assign them a higher security priority. Security support plans address these needs and provide the conduit for the additional security manpower and equipment needed to implement required protection. This approach results in the most efficient use of limited security forces in both peacetime and wartime.
1.7.1. Requesting, Reviewing, and Recommending Security Priorities.

1.7.1.1. If you are the operating MAJCOM of new weapons systems or if you must permanently change the priority of resources, send a coordinated request for priority designation change to HQ USAF/SP. Include the reasons for the priority designation request or change, and specify what the changes mean in terms of personnel, equipment, and facilities as well as what programming (manpower and equipment) actions will be taken to fully implement the new security requirements. **EXCEPTION:** Systems being deactivated do not require a change request. Only notify AF/SP of the deactivation and of the security manpower implications.
1.7.1.2. Air Staff agencies review recommendations for permanent priority designation, assess the Air Force wide implications and recommend approval or disapproval.
1.7.1.3. On the basis of this review, HQ USAF/SP assigns or re-designates the priority.

1.8. Aircraft in Depot Maintenance. Aircraft undergoing depot modification at an air logistics center, contract maintenance center, or which have been turned over to a TDY depot maintenance team for repairs at the operational location, don't retain their formal security priority unless the system security standard specifies otherwise.
1.8.1. Operating and supporting commands ensure depot maintenance environments provide adequate levels of security.
1.8.2. Document depot level security arrangements in support agreements, contract requirements documents, or other appropriate locations.

1.9. Security for Transit Aircraft. When aircraft are in transit (e.g., peacetime operational deployments, public displays, training missions, and air shows), operating commands must provide security equivalent to the security standard. Use the following procedures:
1.9.1. Determine the appropriate level of security, assess the threat, security presence, detection capability, entry control, and alarm response capabilities required by the standard.
1.9.2. The operating command and aircraft commander pre-plan enroute security.
1.9.3. Don't leave aircraft unattended when security is not adequate. Responsible aircrews must guard aircraft until adequate security is in place.
1.9.4. If an aircraft must be left in a location that doesn't have adequate security, aircraft commanders must contact the home base security police (SP) to assist in security arrangements.

1.10. Security Force Capabilities. The security force must detect unusual occurrences, delay and deny entry of unauthorized individuals to the resources, initiate an immediate alarm, provide appropriate armed response, discriminate between hostile acts and other occurrences, and initiate the proper threat condition (THREATCON) and contingency action.
1.10.1. Economy of Force. Employ the security force as economically as possible.
1.10.1.1. Where permitted, an armed security force member posted at an aircraft may perform both aircraft boundary surveillance and entry control duties provided the boundary can be adequately observed.
1.10.1.2. When one restricted area is in close proximity to another and the security forces of one can effectively support both, consider using the security deviation program to document security equivalency and avoid manpower inefficiency.
1.10.1.3. Restricted areas may be large enough to accommodate additional aircraft and maximize the use of already available security forces.

1.11. Restricted Areas. Restricted areas, by definition, contain priority resources. By creating restricted areas, you collect priority resources into defined areas and control them using a single security control system. The DoD (or one of its departments) presides over restricted areas, including portions of civilian airports or other areas that various military departments usually administer.
1.11.1. Definitions. Restricted areas can be:
1.11.1.1. Permanent, to contain priority resources on a continuous basis.
1.11.1.2. Temporary, to contain priority resources for limited periods of time (for example, to park an in-transit priority aircraft).
1.11.1.3. "Limited" and "Exclusion" areas are part of AF restricted areas containing nuclear weapons. For a complete definition of these areas, see DoD 5210.41-M, *Nuclear Weapon Security Manual*, Apr 94.
1.11.2. Authority. The Internal Security Act of 1950 (50 United States Code (U.S.C.) 797) authorizes the DoD to issue regulations to safeguard "property and places." The Secretary of Defense has delegated to military commanders the authority to issue implementing regulations. The AF delegates that authority to "commanders of MAJCOMs, numbered air forces (NAFs), wings, and groups."
1.11.3. Implementing Directive. The installation security regulation forms the foundation for security operations. Each installation possessing or routinely supporting priority resources must have a security regulation. Units may choose to use the installation security regulation to detail other normal security operations. The installation commander must issue, approve, and

assure implementation of the regulation as an installation directive. Publish the regulation as an installation directive. This document:
1.11.3.1. States restricted areas are established "pursuant to DoD Directive (DoDD) 5200.8, *Security of DoD Installations and Resources*, 25 Apr 91 and Section 21, *Internal Security Act of 1950* (50 U.S.C. 797)."
1.11.3.2. States all personnel must obtain specific written permission to enter restricted areas. (Chapter 5 if this instruction depicts specific circulation control requirements.)
1.11.3.3. Designates restricted areas by describing their location and noting that they are marked by warning signs.
1.11.3.4. Establishes entry and internal controls for all restricted areas.
1.11.3.5. Includes a list, in order of importance, of all resources that have a security priority.
1.11.3.6. States the security responsibilities of supporting forces working in restricted areas.
1.11.3.7. Gives the installation chief of security police (CSP) authority to establish security post priority lists and to determine which posts go unmanned during personnel shortages. Specifies that the installation CSP must man posts that directly support nuclear weapons first.
1.11.3.8. Assigns normal security support tasks for units on the installation.

1.12. National Defense Area (NDA). NDAs contain and secure Federal Government resources in US and US territorial areas that don't fall under the jurisdiction of the DoD.
1.12.1. The AF may need to establish an NDA if:
1.12.1.1. Aircraft are sent to civilian airports.
1.12.1.2. An aircraft carrying nuclear weapons makes an emergency landing.
1.12.1.3. It is necessary to immobilize nuclear weapons ground convoys.
1.12.1.4. An aircraft crashes.
1.12.1.5. Other unplanned emergency occur.
1.12.2. Establishing NDAs. Installation commanders, through their on-scene commanders, establish NDAs. Minimum requirements for establishing an NDA are:
1.12.2.1. Use a temporary barrier to mark the boundary of the area.
1.12.2.2. post Air Force Visual Aid (AFVA) 31-101, *Restricted Area Sign-National Defense*, Aug 90.
1.12.2.3. Explain the situation to landowners, including why you need to set up the area and the kinds of controls that are in effect.
1.12.2.4. Get the consent and cooperation of the landowner if at all possible, but establish the area with or without consent.
1.12.2.5. To the greatest degree possible, let civilian authorities handle civilian arrest and detention. If local civil authorities are not present, military personnel may apprehend and detain violators or trespassers. Work with the judge advocate representative to release violators and trespassers to proper authorities.

1.13. Free Zones. Create free zones (zones that contain no priority resources) inside restricted areas when construction projects and similar activities make normal circulation controls inappropriate.
1.13.1. Determining Security Procedures for Free Zones.
1.13.1.1. If a contractor is doing the work, the installation contracting officer gives the contractor a letter signed by the installation commander or the group commander responsible for the security of the area, outlining the contractor's security responsibilities.
1.13.1.2. The USAF organization or agency most directly associated with the project must watch the free zone boundary, provide escorts, and prevent unauthorized entry into the restricted area.
1.13.1.3. For areas containing nonnuclear resources, mark the free zone boundary with an elevated ropes, barriers, fencing, or other suitable materials, to clearly delineate it from the restricted area.
1.13.1.4. Close and secure the free zone at the end of normal working hours.
1.13.2. Areas Containing Nuclear Resources. Free zones contained within areas that have nuclear resources have special procedures.
1.13.2.1. Mark the free zone boundary with a Type B fence.
1.13.2.2. Use personal recognition, entry authority lists (EALs), or installation or military identification (ID) cards to control entry.
1.13.2.3. If it is impossible to create a free zone corridor between the restricted area and the work project area, escort contractor personnel to and from the work area.
1.13.2.4. When necessary to establish a free zone boundary which will temporarily become the boundary of a Priority A area, install a temporary fence which provides the equivalent delay, detection, and physical security deterrence as the permanent fence, including bracing and 45 degree extension arms with three strands of barbed wire. Examples of temporary fencing include:

1.13.2.4.1. The standard type A, 7-foot chain-link fencing.
1.13.2.4.2. A 7-foot high, 6- by 6-inch, 10-gauge mesh, with 4- by 4-inch wood posts.
1.13.2.4.3. A 8-foot high, 11-gauge, chain link mesh, with 2.375-inch outside diameter steel posts set in concrete.

1.14. Installation Security Council (ISC). The ISC is vital to the security planning process. The commander or designee of each installation that supports priority resources appoints the ISC and may combine it with the Resources Protection Committee.
1.14.1. The Council:
1.14.1.1. Selects and designates restricted areas.
1.14.1.2. Ensures that the installation provides adequate personnel, equipment, and facilities for priority resources.
1.14.1.3. Monitors ongoing security enhancement projects.
1.14.1.4. Develops entry-control procedures for free zones.
1.14.1.5. Reviews both the installation security plan and the installation security regulation.
1.14.1.6. Conducts annual reviews of all deviations or waivers in effect.

1.15. Normal Security Operations. The installation security regulation (described in Paragraph 1.11.3) is the basis for normal security operations. Security force planners use it to:
1.15.1. Prioritize post assignments according to the importance of each post to the overall security of the installation's resources.
1.15.2. Determine which posts go unmanned during personnel shortages.
1.15.3. Develop operating instructions. Write detailed instructions that include higher headquarters directives in local procedures. You may base security force checklists on the operating instructions.
1.15.4. Develop security force checklists. Condense long, complicated instructions into concise, step-by-step checklists for security controllers and posted sentries to use.

1.16. Contingency Security Operations. The Installation Security Plan (ISP) is the basic planning document for contingency operations. Contingency plans are those dealing with events likely to occur at your installation.
1.16.1. Publishing ISPs. Installations that routinely manage priority resources must publish this plan.
1.16.1.1. You may combine this plan with the Installation Resource Protection Plan and other related operation plans (OPLANs) into one ISP. Installation commanders issue, approve, and assure implementation of the actions outlined in the ISP.
1.16.1.2. If your unit is an Air Reserve Component (ARC) with a deployment mission, publish a security annex to the host ISP or to the unit mobilization plan showing current in-place plans to secure priority resources.
1.16.1.3. If your ARC unit is a tenant on an installation that doesn't have an ISP, include detailed security arrangement information for the unit in Annex M of the unit's mobilization plan.
1.16.2. Emergency Situations. Be flexible in emergency situations. It's important security planners know which agencies can help during emergencies. When USAF aircraft make emergency or precautionary landings at nonmilitary airfields, the nearest AF installation provides necessary security.
1.16.3. ISP Requirements.
1.16.3.1. Minimally, you must develop a contingency plan for the following events if they apply to your mission:
1.16.3.1.1. Natural disaster.
1.16.3.1.2. Civil disturbance or riot threatening priority resources.
1.16.3.1.3. Overt attack on a restricted area.
1.16.3.1.4. Receipt of threat condition alerting message (TCAM) orders due to a THREATCON change.
1.16.3.1.5. The need to deploy security forces, or to get additional security forces.
1.16.3.1.6. Receipt of Presidential, senior executive mission aircraft (SENEX), specifically designated special air mission aircraft (SDSAM), or special air mission (SAM) aircraft.
1.16.3.1.7. Antihijack.
1.16.3.1.8. Arrival of unidentified or unannounced military or commercial aircraft.
1.16.3.2. Nuclear Weapons Contingency Plans. Installations that support nuclear weapons must also have plans to cover these contingencies:
1.16.3.2.1. Nuclear logistics aircraft support.
1.16.3.2.2. Security force response to accidents or incidents involving nuclear weapons.
1.16.3.2.3. Force generation.
1.16.3.2.4. Nuclear weapons recapture or recovery, including airborne intrusions into areas containing nuclear weapons. (Use CINC or Supported CINC CONPLAN for Counter Proliferation of Capture and Recovery.)
1.16.3.2.5. Overt attack on a nuclear weapons convoy, on- and off-base.
1.16.3.2.6. Department of Energy (DoE) shipment.

1.16.4. Office of Primary Responsibility (OPR). The OPR, designated by each MAJCOM, files the master copy of the ISP and writes the installation's security plan in the appropriate AF or Joint Chiefs of Staff OPLAN format.
1.16.5. Additional Requirements. At nuclear weapons installations, THREATCON procedures must include:
1.16.5.1. Responsibilities of supporting forces (I.E., CE, EMS, and maintenance personnel) working in the restricted area.
1.16.5.2. Conditions and procedures for emergency arming.
1.16.5.3. C3 priorities and procedures between security forces and supporting forces.
1.16.5.4. Expected actions of the supporting forces during all possible scenarios.

1.17. Coordinating With Other USAF Programs. The Air Force Physical Security Program does not stand alone. Planners create an effective security program by coordinating the Air Force Physical Security Program with other major USAF programs such as the Air Force Resource Protection Program in peacetime and the Air Base Defense Program in wartime. This coordinated planning provides a seamless progression of protection programs and completes the installation "security in-depth" picture. Additionally, the Air Force Information Security Program implements DoD guidelines for security of classified information and components in much more cost effective ways than could the Physical Security Program. Other programs also play an important role as noted below.

1.18. Air Force Nuclear Weapons Surety Program. It is important all personnel associated with nuclear weapons security fully understand the relationship between the nuclear weapons surety program and the physical security program because of the overlap between the two. Implement the two-person concept, as outlined in AF 91-series instructions (Safety).
1.18.1. Unoccupied No-Lone Zones. Security force leaders must pair security force personnel posted at unoccupied "no-lone" zones with at least one other security force member. Maintain sufficient forces to be able to prevent unauthorized entry to nuclear exclusion areas early enough to stop any unauthorized arming, launching, firing, or releasing of a nuclear weapon or system.
1.18.2. Responsibilities. The resource user is responsible for the security of no-lone zones that contain only critical components. Persons authorized to enter a no-lone zone without an escort must enforce the two-person concept. Also see **EXCEPTION** in paragraph 1.18.4.
1.18.3. Two-Person Rule Violations. Security force personnel who observe a violation of the two-person concept must report it to central security control (CSC) or missile security control (MSC) and tell the violators to correct the infraction. If the infraction poses an immediate threat to the nuclear weapon or system, security forces clear the no-lone zone and notify the owning or operating agency. Although security forces must be aware of the no-lone zone, they must direct their primary attention to the boundaries of restricted areas and approaches rather than spending their time monitoring compliance with two-person policy rules.
1.18.4. Two-Person Control (TPC) Materials. TPC materials require specific controls defined in Joint Pub 1-04, *Joint Policy and Procedures Governing Positive Control Material and Devices*, Oct 92.
1.18.4.1. The presence of TPC materials has no relationship to the security priority assigned Air Force resources.
1.18.4.2. The presence of TPC materials aboard an unoccupied aircraft does not create a "no-lone-zone" outside of the aircraft, nor does it require application of TPC to the security force. Security forces do not have access to TPC materials.
1.18.4.3. When TPC material is aboard an unoccupied alert aircraft, the security force will enforce TPC by using an air crew list to identify two authorized individuals before allowing entry. Local procedures will identify how the list is prepared and authenticated for the security force.
1.18.4.4. TPC material is not normally left aboard other than primary alert aircraft. Where TPC materials are present on other than primary alert aircraft, their security is normally the responsibility of the unit possessing the material.
EXCEPTION: Primary alert aircraft such as the airborne command posts, have the Airborne Launch Control System (a designated "critical component") on board. Because of this system USAF Safety Rules require the application of PRP and TPC to the supporting security force.

1.19. Security and the Nuclear Weapons Personnel Reliability Program (PRP). You must obtain PRP certification for all security force personnel who directly support nuclear weapons. See AFI 36-2104, *Nuclear Weapons Personnel Reliability Program*.

1.20. Air Force Nuclear Force Security and Survivability (S2) Program.
1.20.1. Program Goal and Objectives. This program is required by *DoDD 3150.3, Nuclear Force Security and Survivability, Aug 16, 1994.* The goal of this program is to improve and maintain the S2 of the AF nuclear force. The objectives of this program include developing programs to enhance the peacetime S2 of nuclear force weapons and their delivery and support systems; developing the capability for rapid dispersal of the nuclear force during transition to war; and improving nuclear force S2 by identifying S2 requirements early in the acquisition process.

1.20.2. Air Force Representation. HQ USAF/SP is the AF representative to the DoD Nuclear Force S2 Steering Group and appoints representatives to the Nuclear Force S2 Working Group.

1.20.3. Programming Responsibility. The Air Force Military Deputy for Acquisition, Office of the Assistant Secretary of the Air Force (Acquisition), has the responsibility for programming and budgeting for research, development, testing, and acquiring S2 systems.

1.20.4. System and Employment Requirements. To meet S2 objectives, MAJCOMs developing requirements and operational concepts for employing nuclear force weapons systems must identify system and employment requirements. SAF/AQ advises the Assistant to the Secretary of Defense (Atomic Energy) how AF S2 are being considered in the acquisition phase.

1.20.5. S2 Evaluation. S2 evaluation of AF nuclear weapons, associated delivery systems, supporting forces, and facilities are conducted via AFI 190-1, *Inspector General Activities*.

1.21. Inspections, Program Exercises, and Staff Assistance Visits. To ensure an acceptable level of security effectiveness, installation commanders must periodically exercise, review, and evaluate the installation security program. These evaluations provide the feedback to determine the validity and scope of security regulations and guidance.

1.22. Inspections. MAJCOMs must perform a variety of inspections simulating peacetime and wartime conditions to determine how ready their security forces are to secure priority resources. Perform these simulations according to safety and inspection directives. Use realistic scenarios to evaluate security forces. Be very careful not to use any scenarios that could be interpreted as an actual hostile situation that might cause accidental injury to personnel or jeopardize the security of priority resources.

1.23. Security Program Exercise (SPE). A security police exercise is a locally initiated exercise that serves as a training session. It lets security and supporting forces walk through THREATCON and contingency actions that they could not otherwise effectively practice during daily operations.

1.23.1. Local Exercises. Conduct local exercises as frequently as needed to maintain a high degree of unit readiness. Every 6 months, exercise at least one THREATCON and contingency action requiring other agency participation.

1.23.2. Contingency Exercise Requirements. MAJCOMs identify the types of contingency actions units must exercise. At least once a year, MAJCOMs must have applicable units exercise the nuclear weapon recapture contingency plan, including those base support actions identified in local plans.

1.24. Force-on-Force (FoF) Training Exercises. FoF training exercises apply to installations possessing nuclear weapons or critical components, those installation supporting prime nuclear airlift force missions (Units providing only Type II security are exempt.), installations supporting layovers of DoE primary safe secure transport, as detailed in Table 2-1 of **technical order (T.O.) 11N-45-51A,** *Transportation of Nuclear Weapons Material*, Oct 91, and are designated by their MAJCOMs.

1.24.1. Scope of Training. Units supporting nuclear weapons must conduct training at least every 12 months. Ideally, have each security force member participate annually. The minimum number of participants for a training operation must equal the number of forces that would normally be involved in such an operation, including the backup force (BF). (See DoD 5210.41-M).

1.24.2. Documenting Training. MAJCOMs must develop procedures for documenting training results.

1.24.3. Training Sites. Units must conduct training in as realistic an environment as possible. MAJCOMS that elect to conduct training where an armed security force is posted will establish necessary policy guidelines. **Never** conduct FoF training where an armed security force is posted and could come in contact with the FoF personnel. When FoF training is conducted within priority resource areas, ensure the actual security force is segregated from the exercise teams. Provide actual security forces with adequate and constant supervision to preclude involvement in exercise scenarios. Provide absolute positive controls to prevent personnel from using live ammunition in the training exercise. All participants must be aware of who is carrying live ammunition. When developing the composition and strategy for the "opposing" force in the FoF training exercises, base your plans on the DoD-postulated threat profile and local or theater-wide threats.

1.25. Staff Assistance Visits. Each MAJCOM must develop an appropriate program to identify and resolve problems and allow responsible base agencies to join in planning and programming actions.

1.25.1. ARC Units. The host installation MAJCOM, the gaining MAJCOM, the National Guard Bureau, and Headquarters Air Force Reserve negotiate agreements for ARC SP units.

1.26. Measuring Compliance with Policy. Compliance with AF physical security policies (see AFPD 31-1) is assessed by measuring incidents involving unauthorized access and damage to priority resources, and deviations from security standards.

1.26.1. Reporting Compliance Data. MAJCOM SP must distinguish between nuclear and nonnuclear assets. Sort deficiencies into raw numbers by category to show trends in unauthorized access and damage to priority resources. Display both categories by priority designation (i.e., A, B, or C.).
1.26.2. Reporting Requirements MAJCOM SP must transmit data to HQ USAF/SPO semiannually by message or letter using report control symbol (RCS): **HAF-SPO(SA)9221,** *Physical Security Deficiencies Report.* Report no later than 31 January and 31 July with a copy to HQ AFSPA/SPS. Don't report during emergencies.
1.26.3. Preparing Reports. To prepare data for the report, use these guidelines:
1.26.3.1. Nuclear Deviations (Approved AF Form 116, Request for Deviation from Security Criteria) by Category:
1.26.3.1.1. Total number of approved temporary deviations (waivers).
1.26.3.1.2. Total number of approved permanent deviations (exceptions).
1.26.3.1.3. Total number of approved technical deviations (variances).
1.26.3.2. Nuclear Deviations (Approved AF Form 116) by type:
1.26.3.2.1. Total number of facility deviations.
1.26.3.2.2. Total number of equipment aid deviations.
1.26.3.2.3. Total number of post and patrol deviations.
1.26.3.2.4. Total number of procedural deviations.
1.26.3.2.5. Total number of other deviations.
1.26.3.3. Nonnuclear Deviations by Category. Use the reporting format in paragraph 1.26.3.1. for nuclear deviations.
1.26.3.4. Nonnuclear Deviations by Type: Use the reporting format in paragraph 1.26.3.2. for nuclear deviations.
1.26.3.5. Unauthorized Access/Damage to Aerospace Resources. Report the number of actual incidents involving unauthorized access and damage to priority resources. Report the:
1.26.3.5.1. Total number of incidents to aircraft, ICBM missile systems, or other priority resources.
1.26.3.5.2. Total number of incidents to equipment located within restricted areas.
1.26.3.5.3. Total number of incidents to facilities located within restricted areas.
1.26.3.5.4. Provide a brief description of each incident.

Chapter 2

DEVELOPING SYSTEM SECURITY STANDARDS

2.1. Overview. This chapter provides instructions for developing system security standard (SSS) to support resources assigned security priority A, B, or C. The ultimate goal of an SSS is to ensure personnel apply a level of security consistent with security priorities to AF resources throughout their life cycle. Use the principles of acquisition security. AFPD 31-7, *Acquisition Security,* provides three processes, each mutually supportable, to aid planners and commanders when developing system security standards.
2.1.1. Program Protection Planning (PPP). The PPP is described in detail in *AFI 31-701, Program Protection Planning.* This process must identify the system's critical elements, threats, and vulnerabilities. The plan represents how the AF plans to protect the system throughout its life cycle. When approved, the plan becomes the authority to apply the security effort it describes.
2.1.2. Systems Security Engineering. Systems security engineering is an element of systems engineering that identifies vulnerabilities by applying scientific principals. This analysis reduces the number of external actions required to eliminate or contain threats to the system. *AFI 31-702, Systems Security Engineering*, explains how to apply this process in detail. Systems security engineering is part of the PPP.
2.1.3. Product Security. Product security addresses the level of protection a system or product requires while located at contractor owned or operated facilities. Program managers determine a security level consistent with the planned security priority of the delivered product or system (*see AFI 31-703, Product Security*).

2.2. System Security Standards. Determining the security priority of a proposed system is an essential part of the PPP process. Program security managers reevaluate this priority when making required changes in the system, its mission, or its capabilities. When making a change in SSS, program security managers must also reevaluate the PPP.
2.2.1. System Security Standard Responsibilities. The operating MAJCOM SP staff must work on the team that develops, reviews, and implements the PPP. They must also participate in the review process on mission need statements, operational requirements documents, and program development plans.
2.2.2. Security Force, Facility, and Equipment Requirements. Program security managers must keep these requirements consistent with the program threat assessment, both in operational and non-operational environments.
2.2.2.1. When applicable, program security managers describe current SSSs in the PPP.

2.2.2.2. When existing SSSs aren't appropriate, the operating MAJCOM must develop a tailored SSS for the PPP.
2.2.2.3. The SSS must include:
2.2.2.3.1. A description of the system or component.
2.2.2.3.2. Any unique operational considerations.
2.2.2.3.3. Security priorities for all phases, including maintenance and resources in depot.
2.2.2.3.4. Unique security-force personnel, facility, equipment, and procedural requirements.

Chapter 3

SECURITY REPORTING AND ALERTING SYSTEMS

3.1. Overview. This chapter describes the purpose of the security reporting and alerting system and procedures for sending reports of unusual security incidents up and down the chain of command.

3.2. Purpose of the System. The security reporting and alerting system defends against widespread, coordinated threats. You can send information about significant security incidents at different locations up or down channels. Higher level headquarters will evaluate and determine the appropriate security-force response.

3.3. Application of the System. The system applies to all USAF installations.

NOTE: THREATCON changes at any USAF installation may interest other installations. When you send a THREATCON increase or decrease message, you must include all MAJCOM/SPs, HQ AFSPA/CC and HQ USAF/SP in the "TO" block.

3.4. Reporting and Alerting Procedures. Local headquarters normally report THREATCON changes. The THREATCON alerting process usually starts at higher-level headquarters and passes down through channels.
3.4.1. THREATCON Change Reporting. You must report THREATCON changes implemented by a local commander or designee as an OPREP-3 BEELINE, according to USAF reporting instructions.

3.5. HELPING HAND Reporting. A HELPING HAND is an unclassified message relayed by CSC to the installation command post of an unusual incident, possibly hostile, affecting priority resources. Incidents are reported to CSC by any means available by anyone who witnesses or discovers the problem. The installation command post shouldn't immediately relay the information to higher headquarters. The security force immediately investigates the situation. **EXCEPTION:** If you believe a hostile event occurred involving a priority resource, immediately up-channel a COVERED WAGON report.
3.5.1. Terminating HELPING HAND Reports. Number HELPING HAND reports sequentially and report in ZULU time. When no hostile event occurred, CSC must request the authority to terminate the HELPING HAND through the installation command post.

3.6. COVERED WAGON Reporting. Initially, a COVERED WAGON report is an unclassified up-channel telephone report (designator immediate or flash) sent up the same communication channel and in the same format as a HELPING HAND report. COVERED WAGON reports inform higher-level headquarters that an unusual incident affecting priority resources, probably or actually hostile, occurred at an installation or dispersed site.
3.6.1. Processing COVERED WAGON Reports:
3.6.1.1. CSC generally sends COVERED WAGON reports to the local command post.
3.6.1.2. The local command post telephones the report to the next-higher-level command post.
3.6.1.3. Each successive command post relays the report, at the same precedence or higher, until it reaches the Air Force Operations Center (AFOC).
3.6.1.4. Report COVERED WAGON incidents as an OPREP-3 BEELINE, according to AF reporting instructions in *AFMAN 10-206, Operational Reports (RCS: HAF-XOO [AR] 7118, OPREP 3--Operational Event and Incident Report).* Include all MAJCOM/SPs, HQ AFSPA/CC, and HQ USAF/SP as an addressee in the "TO" section.
3.6.2 Non-USAF Tenants Installation security planners must work with non-USAF tenants to cooperate and coordinate on THREATCON procedures.
3.6.3. Canceling COVERED WAGON Reports. The installation commander or designee:
3.6.3.1. May cancel the COVERED WAGON. Cancellation may terminate or reduce the THREATCON, depending on the continued threat potential at the installation.

3.6.3.2. Must submit an OPREP-3 BEELINE from the installation command post to report cancellation of a COVERED WAGON.

3.7. Tracking and Evaluating Reports.
3.7.1. Tracking COVERED WAGON Reports.
3.7.1.1. All command levels must log and track COVERED WAGON reports.
3.7.1.2. When the number of active reports indicate coordinated or widespread hostile activities, AFOSC and MAJCOMs must:
3.7.1.2.1. Consult with SP and AFOSI duty officers.
3.7.1.2.2. Issue a Threat Condition Alerting Message (TCAM) out of the MAJCOM headquarters or AFOC.

3.8. Down-Channel Alerting. Evaluating COVERED WAGON reports or current intelligence information may cause an increased state of readiness at a variety of levels. It may affect only one or two installations or installations AF-wide. The TCAM, or down-channel alerting order, sets in motion the increase in readiness posture, as described in Paragraphs 3.8.1 through 3.8.4.:
3.8.1 Transmitting TCAMs.
3.8.1.1. The AFOC or MAJCOM command post electronically transmits the TCAM using a military precedence of IMMEDIATE or FLASH.
3.8.1.2. Use the MAJCOM or USAF abbreviation before the phrase "TCAM" (for example, ACC TCAM; AF-WIDE TCAM).
3.8.1.3. All MAJCOM TCAMs must include all MAJCOM/SPs, HQ AFSPA/CC, and HQ USAF/SP in the "TO" portion of the message.
3.8.2. USAF Tenant Organizations on Non-USAF Installations. Local AF planners must establish written procedures that secure USAF resources at the appropriate level in the event of a TCAM.
3.8.3. Implementation. As a rule, TCAMs don't trigger a theater-wide or AF-wide THREATCON. They must give a summary of the situation and offer a recommended course of action. Commanders then tailor responses to local situations rather than mandating across-the-board actions.
3.8.4. Implementing a THREATCON as a Result of a TCAM. When the TCAM directs a THREATCON, you must implement it. A THREATCON implemented in response to a TCAM remains in effect until the originating or higher-level authority, cancels it.

3.9. Security Police Lessons Learned. The security police lessons learned program is devised to crossfeed information between commanders and managers throughout the career field. This program culminates in a living document managed by HQ AFSPA/SPSS. Commanders are urged to provide lessons learned on situations occurring within their units. It is important to gain this valuable information to create a data base of guidance information for future planning. Reporting requirements are contained in AFI 31-209, Chapter 13 and Attachment 3. The point of contact for all lessons learned information is HQ AFSPA/SPSS at DSN 263-0067.

Chapter 4

THE SECURITY DEVIATION PROGRAM

4.1. Overview. The security deviation program formalizes security program risk acceptance. The inability to meet minimum DoD and Air Force Physical Security Program requirements results in a higher security program risk. All units which accept a higher risk than established by regulation must implement the security deviation program. The deviation program:
4.1.1. Ensures units comply with the security standards for specific weapons, weapons systems, and facilities.
4.1.2. Provides a management tool for units and MAJCOMs to review and monitor corrective actions. (See DoD 5210.41-M for additional information for units supporting nuclear weapons.)

4.2. Categorizing Deviations. Categorize deviations as a permanent deviation (exception), temporary deviation (waiver), or a technical deviation (variance).
4.2.1. Permanent Deviations (Exceptions). Request a permanent deviation or exception when a security-threatening condition that can't be corrected exists or when correcting a problem would cost too much. Conditions approved as permanent deviations require compensatory measures and have no expiration dates.
4.2.2. Temporary Deviations (Waivers). Units request a temporary deviation or waiver when a correctable, security-threatening condition exists. Conditions approved as temporary deviations require compensatory measures. Grant temporary

deviations for no more than 1 year for restricted areas containing nuclear weapons and no more than 2 years for nonnuclear support areas. Consider subsequent requests for temporary deviations as extensions.
4.2.3. Technical Deviations (Variances). Units request a technical deviation or variance when a condition exists that doesn't threaten security but technically differs from specifications in the directive. Conditions approved as technical deviations don't require compensatory measures or corrective actions.

4.3. Reviewing, Approving, or Disapproving Deviations from Nuclear Security Standards. If the unified commander doesn't choose to exercise deviation authority over AF and subordinate supplemental nuclear security standards, send deviation requests to the MAJCOM responsible for security.
4.3.1. Approving Authority. The MAJCOM commander or general officer on the staff reviews and approves or disapproves deviation requests.

4.4. Reviewing and Approving, or Disapproving Deviations from Nonnuclear Standards. MAJCOMs specify the level of review, approval, or disapproval of deviation requests for nonnuclear security standards.
4.4.1. Routing Deviations.
4.4.1.1. Send deviations involving the security of tenant unit resources through host command channels to the tenant MAJCOM headquarters for coordination.
4.4.1.2. MAJCOMs:
4.4.1.2.1. Address the deviation approval process in MAJCOM supplements for units located on another MAJCOM's installation.
4.4.1.2.2. Correspond with the tenant's MAJCOM to coordinate deviation procedures.
4.4.1.3. When installation commanders or NAF staffs approve deviations, they forward a copy of the deviation to NAF or MAJCOM, as applicable.

4.5. Compensating for Deviations. Units must compensate for the specific security threat created by a deficiency.

NOTE: Security forces, facilities, equipment, and procedures that are already required to serve a priority resource don't qualify as compensatory measures. Instructions that consist mainly of orders to "increase vigilance" are also insufficient.
4.5.1. Applying Compensatory Measures. Security force supervisors must inform security forces of the deviations in their assigned areas and instruct them on required compensatory measures. Compensatory measures may includes additional:
4.5.1.1. Procedures.
4.5.1.1.1. Facilities.
4.5.1.1.2. Equipment (such as additional locks, intrusion detection systems (IDS), lighting, and barricades).
4.5.1.1.3. Security forces that provide an equal level of security.
4.5.2. Compilation of Deviations. Consider all other deviations when requesting and approving deviations to prevent a combination of individual deviations from creating an overall security problem. Collectively, deviations must not cause more of a security threat than the problems they were originally designed to solve.

4.6. Documenting Deviations. Document deviations on AF Form 116 and submit each deviation for formal approval. **EXCEPTION**: Don't apply for formal approval if the directive from which you are deviating specifically states it isn't necessary.
4.6.1. When Deviations Aren't Required. Don't apply for a formal deviation if:
4.6.1.1. You deviate by 10 percent or less from the measurable standards for fencing, lighting, clear zones, distance between fences, or from another requirement.
4.6.1.2. You change manning of nonnuclear posts during temporary personnel shortages.
4.6.1.3. You can correct nonnuclear deficiencies within 60 days of finding the problem.

NOTE: The unit that finds the deficiency must notify the approving authority and compensate for the problem.

PART 2
APPLYING THE PHYSICAL SECURITY PROGRAM--PROCEDURES, FORCES, FACILITIES, AND EQUIPMENT

Chapter 5

RESTRICTED AREA CIRCULATION CONTROL PROCEDURES

5.1. Overview. This outlines procedures for controlling circulation in restricted areas. Circulation controls:

5.1.1. Prevent unauthorized entry.

5.1.2. Detect hostile actions within the area.

5.1.3. Counter the introduction of hazardous materials into the area.

5.1.4. Prevent unauthorized removal of material from the area.

5.1.5. Meet the investigative requirements in *AFI 31-501, Personnel Security* and the suitability guidelines located in *DoD 5200.2-R, Appendix I, Personnel Security Program.*

5.2. Unescorted Entry. Never grant unescorted entry solely to avoid the inconvenience of escorted entry. Use AF Form 2586, *Unescorted Entry Authorization Certificate*, to document, coordinate, and approve unescorted entry authority.

5.2.1. Completing AF Form 2586.

5.2.1.1. The individual's unit commander or designee completes Sections I, II, III, and Columns 1, 2, and 3 of Section IV. Signature of the unit commander or designee in Section II certifies that all available records were reviewed and contain no disqualifying information. When completing Column 2 (escort official) of Section IV, indicate whether the individual has escort authority by typing "Yes" or "No" in this block.

5.2.1.2. The approving official completes the applicable portions of section IV.

NOTE: The installation commander designates approving officials for each area by naming their positions in the installation security regulation. Installation commanders may designate SP unit commanders as approving officials for security force members.

5.2.1.3. Approving officials type or print their names in the signature blocks and sign the forms. Approving officials who sign Section IV also serve as the approving officials for unescorted entry and escort authority, if applicable.

5.2.1.4. Designees may not grant themselves unescorted entry.

5.2.1.5. Use a form of signature verification (i.e., DD Form 577 or letter showing sample signatures) for those persons signing sections II and IV.

5.3. Issuing, Inventorying, and Disposing of Badges.

5.3.1. Issuing Badges.

5.3.1.1. The individual applying for unescorted entry carries the completed AF Form 2856 to the badge-issuing official.

5.3.1.2. The badge-issuing official completes Section V, authenticates it, and issues the restricted area badge (RAB). Only individuals assigned to the badge-issuing activity and appointed in writing by the installation CSP may act as issuing officials.

5.3.1.3. The RAB serves as an official document and shows the bearer's photograph, signature, and other pertinent ID data. For each badge, issuing officials:

5.3.1.3.1. Indicate "grade" on the badge by OFF (officer), ENL (enlisted), CIV (civilian), OSI (AFOSI special agents), ART-OFF (Air Reserve technician-officer), ART-ENL (Air Reserve technician-enlisted).

5.3.1.3.2. Enter the last six numbers of the bearer's social security number (SSN) in the block marked "SSN."

5.3.1.3.3. Block out unused numbers on the badge to show specific restricted areas on the installation where the bearer may not enter unescorted.

5.3.1.3.4. Mark the badge with a locally devised authenication feature before laminating it.

5.3.1.3.5. If the bearer serves as a designated escort official, type or stamp a capital letter "E" to the right of the numbers 1 to 10 or to the left of numbers 11 to 20 to show the restricted area where the bearer may perform escort official duties.

5.3.1.4 Restricted area badges may be coded either electronically for use with AECS or physically on the AF Form 1199 for level of security clearance, PRP status, and special access programs, however; don't use specific terms which are visible on the form such as PRP, top secret, secret, etc. Do not use the badge as the sole verification to grant access to classified information. Units may distinctly mark the exchange badge of persons authorized unescorted entry into restricted areas containing nuclear resources who do not perform duties directly associated with the nuclear weapons system, i.e., grounds maintenance, vending, and administrative personnel.

5.3.2. Using Badges in Restricted Areas. MAJCOMs may allow personnel to use RABs for controlled area or installation entry if the badges are otherwise required for restricted area entry.
5.3.2.1. For AF reserve members who have dual status as Federal employees on base, issue one AF Form 1199 series badge showing both the civilian and reserve requirements. In the grade block of AF Form 1199, indicate "CIV/ENL" or "CIV/OFF." Ensure that both the civilian and reserve units have copies of AF Form 2586. Reissue the badge if the individual separates from either position.
5.3.2.2. The installation security regulation will list the unit responsible for initiating the AF Form 2586.
5.3.2.3. The original AF Form 2586 is returned to the badge requesting organization where it is kept on file.
5.3.3. Supplying USAF RABs. Badges are numbered serially and color coded.
5.3.3.1. AF Form 1199, **USAF Restricted Area Badge (Blue).**
5.3.3.2. AF Form 1199A, **USAF Restricted Area Badge (Green).**
5.3.3.3. AF Form 1199B, **USAF Restricted Area Badge (Pink).**
5.3.3.4. AF Form 1199C, **USAF Restricted Area Badge (Yellow).**
5.3.3.5. AF Form 1199, CD, **USAF Restricted Area Badge (Computer Generated).**

NOTE: Security police obtain badges from the servicing Publications Distribution Office.
5.3.4. Storing RABs. Badge issuing officials store blank badges in a locked steel cabinet or somewhere more secure.
5.3.5. Inventorying Badges. Badge issuing officials inventory each badge by serial number and advise the sender of any discrepancies. Log each series of forms on separate copies of AF Form 335, **Issuance Record - Accountability Identification Card.** Enter each badge serial number in Column A and the local badge number, if used, in Column D, re-titled "local badge number." Attach AF Form 213, **Receipt for Accountable Form,** along with reports of investigations for lost badges and certificates of destruction. To record destruction use a letter or Air Force general purpose form. Ensure the following minimum information is recorded: all badge numbers destroyed, date of destruction, and signature of an authorized destruction official.

NOTE: Secure automated badge making materials (card stock and specially marked laminates) as per paragraph 5.3.4. above.
5.3.6. Reporting Missing or Lost Badges.
5.3.6.1. If badge issuing official finds a blank badge missing, the installation CSP must conduct a thorough investigation to determine the reason for the loss.
5.3.6.2. If badge issuing officials can't issue a blank badge, they mark AF Form 335 to show why they can't issue the badge.
5.3.6.3. If the bearer loses the badge, the commander or designee investigates the loss and sends a copy of the report to the badge-issuing official. Investigate and report the loss before reissuing a badge.
5.3.6.4. The SP issuing official destroys surrendered or confiscated badges immediately and records destruction as indicated in paragraph 5.3.5.
5.3.6.5. Commanders must account for any confiscated badges held pending a final decision to disqualify personnel.
5.3.7. Auditing In-Stock Badges.
5.3.7.1. The installation CSP must appoint a commissioned officer or senior noncommissioned officer (NCO) to audit all badges in stock annually.
5.3.7.2. Issuing officials must inventory in-stock badges before a new official takes charge. During an audit or inventory, use AF Form 335 to account for issued badges.
5.3.8. Reissuing Badges.
5.3.8.1. Bearers report damaged or indistinct badges to their unit commander. Bring the original copy of AF Form 2586 and the original badge to the badge-issuing activity.
5.3.8.2. Badge-issuing activities issue the bearer a new badge and mark the badge number on all copies of AF Form 2586.
5.3.8.3. Reissue all badges for an installation or area when a compromise of the badge system is indicated or the commander loses confidence in the system. Follow the procedures for individual reissue when reissuing badges for the entire installation.
5.3.9. Disposing of Badges.
5.3.9.1. When badge bearers leave an installation for another assignment or separate, because of a discharge, or to retire, unit commanders or designees ensure that they hand carry their badges and the original copy of AF Form 2586 to the badge-issuing office at least one workday before leaving.
5.3.9.2. The badge-issuing office must receive all personnel departure notices and establish a suspense system for departing personnel's badges and copies of AF Form 2586.
5.3.9.3. Security police must retrieve exchange badges. Destroy all badges on or before the date listed in the departure notice. **EXCEPTION:** Unit commanders or designees may delay a departure date and propose a new one in writing or by telephone.
5.3.9.4. Unit commanders must ensure that badges issued to a bearers whose entry authority is permanently withdrawn are returned immediately to the badge-issuing office.
Form 2586 as prescribed by AFI 31-501, *Personnel Security*.

5.3.10. Adding Areas on the Badge.
5.3.10.1. When reissuing a badge to add an area, annotate the remarks section of the original copy of AF Form 2586 at the bearer's unit, "Add area X" and include the name and signature of the individuals commander. Add the new area in Section IV and ensure normal area coordination is accomplished. If the AF Form 2586 remarks section does not have sufficient space to annotate, complete a new AF Form 2586.
5.3.10.2. The bearer hand carries the original badge, the newly annotated original copy of the AF Form 2586, and a copy of the newly annotated AF Form 2586 to the badge-issuing activity. The badge-issuing activity verifies the form and issues the new restricted area badge.
5.3.10.3. The badge-issuing activity files a copy of the new AF Form 2586 with the previous AF Form 2586 maintained within the badge-issuing activity.
5.3.11. Deleting Areas on the Badge.
5.3.11.1. When reissuing a badge to delete an area, the individual's unit commander or designee annotates the original copy of AF Form 2586, "Delete area X". If the AF Form 2586 remarks section does not have sufficient space to annotate, complete a new AF Form 2586. to the badge-issuing activity.
5.3.11.2. The bearer hand carries the old badge, the annotated original copy of the AF Form 2586, and a copy of the newly annotated AF Form 2586 to the badge-issuing activity. The badge-issuing activity issues a new restricted area badge minus the deleted area.
5.3.11.3. On all copies of AF Form 2586, the badge-issuing activity:
5.3.11.3.1. Adds the new badge number, strikes out the deleted area, and marks the form, "deleted, per attached letter."
5.3.11.3.2. Files a copy of the newly annotated AF Form 2586 with a copy of the old AF Form 2586..

5.4. Maintaining AF Form 2586. File the original copy of AF Form 2586 at the requesting unit until the bearer surrenders the badge. Each unit must establish the number of copies of AF Form 2586 required.

5.5. Establishing Temporary Badging Systems. MAJCOMs may establish procedures for implementing temporary badging systems that allow unescorted entry to authorized personnel for a short period of time. Use this system at nonnuclear restricted areas where no advanced entry control system (AECS) exists. Refer to paragraph 5.15 for AECS procedures.
5.5.1. Requirements for Temporary Badging Systems. Temporary badging systems must:
5.5.1.1. Use distinctly marked RABs (AF Forms 1199) to identify badge holders with temporary unescorted entry.
5.5.1.2. Require positive ID at the entry control point (ECP).

NOTE: The badge must never leave the restricted area for which it is authorized.
5.5.1.3. Ensure that individuals given badges authorizing unescorted entry have no disqualifying records under the industrial, personnel, or information security programs.

NOTE: Don't use a temporary badge as a 1-day substitute for lost or forgotten badges. Replace lost or forgotten badges with visitor badges that require an escort.
5.5.2. Making Temporary Badges. Don't fabricate or create homemade badging systems - they defeat the approval and coordination process.
5.5.3. Authorizing Unescorted Emergency Entry. The installation commander or designee may authorize unescorted emergency entry into restricted areas based on available evidence of the individual's known trustworthiness. Before issuing the restricted-area badge, note "Emergency unescorted entry required," followed by a brief explanation in the remarks Block of AF Form 2586.

5.6. Controlling Unescorted Entry--General Techniques. Personnel may use RABs at more than one installation for unescorted entry when the badge is used with a valid EAL. Establish identities and levels of authority according to instructions in paragraph 5.12.2.

NOTE: Personnel must remove restricted area badges when not within a restricted area.

5.7. Controlling Unescorted Entry With Exchange Badges.
5.7.1. Issuing Exchange Badges. Issue two badges for each person authorized unescorted entry. Issue the basic badge according to paragraph 5.3. Issue the second, or exchange badge, with information identical to that on the basic badge but on a different color paper stock. Mark the exchange badge only with the number for the authorized restricted area. See AFI 31-101, volume 2, paragraph 2.
5.7.1.1. Two people must review and verify all issue data before badge manufacture.
5.7.1.2. Verify the AF Form 2586 is valid (e.g., via signature card or similar method).

5.7.1.3. Positively identify the badge applicant using picture ID and an independent source (e.g., base personnel roster).
5.7.1.4. Provide two person control over exchange badge stock.
5.7.2. Using Exchange Badges.
5.7.2.1. Personnel from the security force or badge-issuing officials must hand carry exchange badges directly to the entry controller (EC).
5.7.2.2. Exchange badges at the entry control facility (ECF) may be marked or numbered to help personnel track them during exchange and inventory.

NOTE: Don't mark or number the basic badge. If the badge is lost or stolen, such a mark or number could compromise the system.
5.7.2.3. During the exchange (entering and leaving), the EC compares:
5.7.2.3.1. The basic and exchange badges to make sure that they contain identical information.
5.7.2.3.2. The photographs on the badges with the bearer.
5.7.2.4. The EC maintains strict accountability for the exchange badges by checking and inventorying all badges maintained at the ECF at the beginning of each shift. Record badge deletions and additions.

5.8. Using Single Badges. This entry control technique requires only one badge for each person with authorized unescorted entry into a restricted area. The EC compares the photograph and other identity data on the badge with the bearer's physical characteristics. **CAUTION:** The single badge technique is relatively easy to defeat. Use one of these supporting techniques to reinforce its effectiveness:
5.8.1. Personal Recognition. Use personal recognition after the EC has initially verified the individual's authority to enter the restricted area.
5.8.2. Checking Signatures and Credentials. Ask the bearer to produce a personal ID credential (DD Form 2, **U.S. Armed Forces Identification Card**, for instance) with a picture and signature. Compare this with data on the RAB.
5.8.3. Entry Authority Lists (EALs). Compare entry credentials with information contained on the entry authority list. Ensure accuracy between the two documents.
5.8.4. Verifying Entry Authority by Telephone or Radio.
5.8.4.1. Designated unit dispatching agencies or similar authorities notify CSC security controllers when a person needs to enter an area.
5.8.4.2. Security controllers verify that they received the notification and inform the area EC of the impending entry.
5.8.5. Sign and Countersign. Establish a sign that personnel must give in order to pass through an area in reply to another sign. Use these signs and countersigns to facilitate entry into restricted and close-in areas during alert force launches and emergencies.

5.9. Using Duress Codes. A duress code is a word or words used during normal conversation to indicate duress. Protect the code by revealing it only to those who need to know it, physically safeguarding it, and changing it every 6 months or when compromise is suspected.
5.9.1. Establishing Duress Codes.
5.9.1.1. All armed security force members must know the duress code.
5.9.1.2. All personnel with unescorted entry authority working in support of nuclear resources must know the duress code.
5.9.1.3. MAJCOMs decide when other personnel working in nonnuclear support areas need to know the duress code.

5.10. Requirements for Unescorted Entry to Areas that Contain Nuclear Resources. Use the most stringent unescorted entry controls for restricted areas containing nuclear resources.
5.10.1. Security Forces: See also AFI 31-101, volume 2, paragraph 2.
5.10.1.1. Use an exchange badge system to identify and admit personnel with authorized unescorted entry.
5.10.1.2. Conduct searches according to the procedures described in DoD 5210.41-M.
5.10.1.3. Prohibit privately-owned vehicles from driving into or parking in restricted areas and external clear zones. See DoD 5210.41-M for vehicle inspection requirements.
5.10.1.4. MAJCOMs specify under what circumstances drivers must accompany security force members performing the inspection.
5.10.1.5. Open both gates for convoys, emergencies, or oversized vehicles only. Post an armed guard in the entrapment area when both gates are open.
5.10.2. Entering No-Lone Zone Security Areas.
5.10.2.1. The Security Force:
5.10.2.1.1. Ensures that people with authorized entry properly identify themselves before entering no-lone zones.

5.10.2.1.2. Grants entry to at least two people to a previously unoccupied no-lone zone.
5.10.2.1.3. Need not control entry into no-lone zones that don't contain nuclear weapons.
5.10.2.2. A single, designated vouching authority approves subsequent entry into occupied no-lone zones. (A designated vouching authority is the individual who approves entry into an occupied exclusion area. He or she meets suitable two-person team requirements and exercises control of the exclusion area.)
5.10.2.3. MAJCOMs may prescribe more detailed procedures in their supplements to this instruction.
5.10.3. Entering Storage Structures.
5.10.3.1. Authorized munitions maintenance personnel approve entry into storage structures. Notify the security force of such authorization in writing.
5.10.3.2. Individuals authorized to approve entry must use authentication and duress procedures and pre-announce entries. See AFI 31-101 Volume 2, paragraph 2.
5.10.3.3. Before opening or closing storage structures, two designated maintenance personnel must contact the master surveillance control facility operator (MSCFO) or alarm monitor and identify themselves using an authentication code.
5.10.3.4. Security force planners must ensure that a duress system is available during opening and closing procedures. *EXCEPTION:*If alarms are inoperative or haven't been installed, two designated maintenance personnel must present themselves to a security force member and identify themselves before opening and closing.
5.10.3.5. Alarm monitors tell security forces in the area the identity of maintenance personnel and where they are authorized to enter.
5.10.3.6. The alarm monitor or MSCFO must record all openings and closings of structures containing nuclear weapons.
5.10.3.7. Munitions maintenance personnel usually serve as armed guards for unlocked structures.
5.10.3.8. Alarm response teams (ARTs) may watch approaches to open structures containing nuclear weapons if their response capability is not degraded.
5.10.3.9. Security planners must ensure that communications are available to alert personnel at the open structure of imminent danger and to notify munitions personnel when the ART discontinues surveillance to perform response duties.
5.10.4. Entering Alert Aircraft Shelters and Bomber Aircraft No-Lone Zones. Follow the procedures in SSSs, MAJCOM directives, or installation contingency plans.
5.10.5. Unescorted Entry into Restricted Areas Containing Nonnuclear Priority Resources. Use an approved badge system and one or more of the supporting techniques in paragraphs 5.8.1 through 5.8.5 to identify people requesting entry.
5.10.5.1. Security Personnel:
5.10.5.1.1. Need not inspect vehicles and hand-carried possessions.
5.10.5.1.2. Prohibit privately-owned vehicles from driving or parking in permanent restricted areas with nonnuclear priority A and priority B alert aircraft or parking in external clear zones.

5.11. Using Escorted Entry Procedures.
5.11.1. Overview. Escorted entry is used to allow people with an official need to enter restricted areas but who are not authorized unescorted entry.
5.11.1.1. The Installation Commander:
5.11.1.1.1. Designates escort officials by signing the approving official's signature block in section IV of the AF Form 2586 for each area where escort official authority is granted. **EXCEPTION:** Missile wings and groups may use a MAJCOM prescribed form.
5.11.1.1.2. May designate individual duty functions, such as aircraft maintenance team chiefs and weapons load crew chiefs and give these people authorized escort authority in the installation security regulation.
5.11.1.2. Escort Officials. Escort all people without unescorted entry authority. Escort officials assume responsibility for the safe and secure conduct of visitors and personally keep visitors under surveillance and control or designate an escort to do so. Escort official must brief visitors on security rules before they enter the restricted area. Local security forces work with owners and users to develop the visitor briefing.
5.11.2. Training Escorts and Escort Officials. Conduct this training as part of Phases I and II, Physical Security Awareness Training. Use a locally devised lesson plan and test to train and formally certify escort officials. Recertify escort officials annually and when any significant change occurs in visitor procedures.

5.12. Visiting Restricted Areas. Visitors are personnel who are not assigned to the installation and do not possess a recurring need to enter a restricted area. When these personnel visit Priority A (Nuclear and Non-nuclear) and Priority B areas, an entry authority list (EAL) must support the visit. (See paragraphs 5.5 (5.15 for AECS systems) and 5.6 for visitors with an official need for unescorted entry to the restricted area, e.g., FCDNA, MAJCOM and NAF inspection or staff assistance teams.) Post EALs at applicable entry control points and/or CSC. Installations maintain this list as a computer product, card file, AF Form 2586 file, message, or letter. EALs may be provided via secure data automation networking systems operating

at points between pass and registration and ECFs. Use a formal procedure for authenticating and distributing EALs through a security-force supervisor.

5.12.1. Units may reproduce EALs; however, EALs in support of restricted areas containing nuclear resources must show an original authenication signature from the security force supervisor.

5.12.2. For all authorized personnel, EALs must include:

5.12.2.1. Name, rank, and last six numbers of the SSN.

5.12.2.2. Organization.

5.12.2.3. Badge number.

5.12.2.4. Clearance status.

5.12.2.5. Dates of visits (if applicable).

5.12.2.6. Expiration date.

5.12.2.7. Individuals assigned to the installation, and who need escort to perform official duties within the restricted area, are not considered visitors but must be processed as outlined in paragraph 5.12.4.

5.12.3. Visit Requests. Visitors need specific approval before escort into restricted areas. Individuals visiting restricted areas:

5.12.3.1. Must formally request approval beforehand.

5.12.3.2. Address the request to the installation commander with information copies to the appropriate MAJCOMs and intermediate headquarters.

5.12.3.3. The installation commander can delegate visit approval authority to the approving official identified in Paragraph 5.2.1.3.

5.12.3.4. Send information copies of requests to Munitions Squadrons (MUNS) (formerly Aviation Depot Squadrons) to the 377th Logistics Group, 4600 Randolph Ave., SE, Kirtland AFB NM 87117-5850. All visit requests must include:

5.12.3.4.1. Name, SSN, and rank.

5.12.3.4.2. Duty title.

5.12.3.4.3. Clearance status.

5.12.3.4.4. Military, Government, or civilian agency affiliation.

5.12.3.4.5. Date of the proposed visit.

5.12.3.4.6. The host-installation agency sponsoring the visit.

5.12.3.4.7. Reason for the visit.

5.12.4. Escorting Visitors in Restricted Areas Containing Nuclear Weapons.

5.12.4.1. Visitors must make arrangements in advance. Develop local procedures to assure escorted individuals have a valid official reason to enter the area. See AFI 31-101 Volume 2, paragraph 2. Verify the need for visit through a means independent of the escort (e.g., work control centers, local visit approval process, etc.).

5.12.4.2. Before allowing a visitor to enter the entrapment area, the EC and escort official must establish:

5.12.4.2.1. The visitor's identity. Maintain a record of the visit on the AF Form 1109, **Visitor Register Log**.

5.12.4.2.2. Purpose of the visit.

5.12.4.2.3. Duration of the visit.

5.12.4.3. Security police units must develop procedures to ensure all visitors are screened by or pass through a metal detector before they enter. Security police units must develop procedures to ensure all visitors are screened by or pass through a metal detector before they enter. **EXCEPTION:** The installation commander or group commander responsible for security of the area may exempt specific visitors from the metal detector screening.

5.12.4.4. Visitors are not normally authorized to bring handcarried items into restricted areas. The installation commander or group commander responsible for security of the area approve, on a case-by-case basis, authority for visitors to hand-carry items into and out of the restricted area.

5.12.4.5. A security force member must inspect any hand-carried possessions and any vehicles before visitors enter or leave the restricted area. Escort officials may assist.

5.12.4.6. The agency or person sponsoring the visit must safeguard items that aren't allowed into the area.

5.12.4.7. The installation commander or group commander responsible for security of the area may deem it necessary to use armed escorts.

5.12.5. Requirements for Field Command Defense Nuclear Agency (FCDNA) Inspectors.

5.12.5.1. Authority for FCDNA inspection teams to enter restricted areas is based on three items:

5.12.5.1.1. A valid Defense Nuclear Agency (DNA) Form 442, **Security Identification Badge**, Jul 81, or FCDNA 239, Apr 86.

5.12.5.1.2. A valid military ID card.

5.12.5.1.3. Identification information appearing on their electronically transmitted inspection notices.

NOTE: The team may handcarry an updated version of their EAL and present it to the commander of the inspected unit upon arrival.

5.12.5.2. The DNA Form 442 and FCDNA 239 are red badges with the bearer's name and photograph on the front. The badge number and validating official's signature appear on the back.
5.12.5.3. FCDNA's electronically transmitted inspection notification must include the name, rank, SSN, and badge number.
5.12.5.4. The installation commander or group commander responsible for security of the area must sign the FCDNA's inspection team EAL and indicate which areas the team may enter.

NOTE: Inspection team members may not be assigned as the second member of a two-person concept team as defined in AFI 91-101, *Air Force Nuclear Weapons Surety Program.* They must be escorted by an authorized two-person team when entering an exclusion area. Ensure that the original signed inspection notification is kept in CSC/MSC for the duration of the inspection as the original, master EAL.
5.12.5.5. All personnel use copies of the master EAL, authenticated by a SP supervisor, as an official EAL at each restricted area entry point.
5.12.6. Escorting Visitors into Restricted Areas Not Containing Nuclear Weapons.
5.12.6.1. Visitors need not make arrangements in advance. Visitors need not make arrangements in advance. **EXCEPTION:** MAJCOMs may require that certain visitors make advance arrangements.
5.12.6.2. Before allowing entry, the EC and escort official must establish the visitor's:
5.12.6.2.1. Identity. Maintain a record of the visit on the AF Form 1109. **EXCEPTION:** A record of the visit need not be maintained for areas containing only priority C resources.
5.12.6.2.2. Reason for entering.
5.12.6.2.3. Duration of stay.
5.12.6.3. For restricted areas containing only priority C resources, all individuals with a RAB for the area may act as escort officials. Escort officials inspect the visitor's vehicle and certifies to the EC, if assigned, that the inspection was conducted.
5.12.6.4. MAJCOMs may require departure inspections and prescribe search policies for visitors' hand-carried possessions.

5.13. Requirements for AECS. Use these electronic systems to enhance the ability of the security force to positively identify individuals who wish to enter restricted and controlled areas. AECS is a subsystem of the overall security sensor system. Develop a manual back-up system to control entry if the AECS system fails. For approval and certification procedures, see those prescribed in chapter 8 for sensor equipment. Before purchasing and installing AECS, obtain approval from HQ USAF/SP.
5.13.1. Requirements for AECS Equipment. The AF divides AECS into three levels, all based on AF Form 1199, **CD, Air Force Entry Control Card (Blue)** and an electronic card reader. All areas may use AF Form 1199, CD. Those units previously authorized to use locally fabricated or contractor form cards must use AF Form 1199, CD or computer generated equivalent when the system is replaced. All new systems installed after 1 Jan 94 must use AF Form 1199, CD, or a contractor-supplied computer generated equivalent. Computer generated badges must meet the requirements outlined in paragraphs 5.3.1.3, 5.13.5, and 5.14.
5.13.2. Using Level I. Use level 1 systems to control entry to controlled areas and some restricted areas containing only priority C resources. The AF Form 1199, CD, when passed through the card reader, compares personal information encoded on a magnetic stripe to a controlled computer database to verify authority to enter the area. Once verified, the individual may proceed. A level 1 system uses a credential reader to read entry data encoded on the RAB.
5.13.3. Using Level II. Use Level II systems for most restricted areas containing priority B and C resources and some nonnuclear priority A resources when you have additional internal controls in place. Level II uses a personal identification number (PIN) in addition to the card and card reader. When you pass the card through the card reader, it compares the personal information on the stripe and the PIN for a match in the database. Once verified, the individual may proceed.
5.13.4. Using Level III. Use level III systems for restricted areas containing priority A and certain priority B resources. For permanent areas containing nuclear weapons, you may use Level III AECS in place of a exchange-badge system. In addition to the card, card reader, and PIN, this level adds another verifier. The added verifier is a personal trait, such as hand geometry or the pattern of blood vessels on the retina. When you pass the card through the reader, the system assesses and verifies the PIN and the personal traits. Once verified, the individual may proceed.
5.13.4.1. Entry Control Booths. Establish a maximum weight tolerance of +/- 25 pounds when configuring both weight-checks. This will allow for the weight differential associated with adverse weather clothing and/or reasonable weight gain or loss.
5.13.5. Using Card Readers. Security system programmers must use:
5.13.5.1. A card reader that is compatible with AF Form 1199 CD, and can accept high coercivity magnetic stripe (4000 Oersteds), American Banking Association Track Two, 75 bits per inch, 5 bits per character, 40 characters.
5.13.5.2. Credential programming equipment to encode the restricted area badge. Contact HQ ESC/AVJD, 20 Schilling Circle, Hanscom AFB MA 01731-2816 for coding information. The card writer must format:

5.13.5.2.1. Agency Code. A four-digit code on all credentials identifying the agency to which the card holder is assigned (for example, 0001 - USAF; 0002 - US Army; 0003 - US Navy; 0004 - US Marine Corp).
5.13.5.2.2. System Code Number. A four-digit field, unique to each AF installation, identifying the system in which the card is enrolled.
5.13.5.2.3. Credential Number. A six-digit code assigned to each card by the issuing agency. No duplicate numbers must be simultaneously active.
5.13.5.2.4. Series Number. A single-digit field that reflects major system changes.
5.13.5.2.5. Individual Credential Number. A single-digit field, initially encoded as "1," which increases incrementally every time a badge is replaced due to loss or damage (the replacement badge is "2," its replacement is "3," and so on).

5.14. Issuing and Manufacturing AECS Badges. To issue AECS badges, use the guidelines in paragraph 5.3.
5.14.1. The following procedures apply to manufacturing AECS badges. See AFI 31-101 Volume 2, paragraph 2.
5.14.1.1. Develop local procedures to control the manufacturing process.
5.14.1.2. Verify the AF Form 2586 is valid (e.g., via signature card or similar method).
5.14.1.3. Positively identify the badge applicant using picture ID and another independent source (e.g., base personnel roster).
5.14.1.4. The AF requires system software or procedures that incorporate the two-person verification method so that only two people who meet the requirement may enter database information.
5.14.1.5. MAJCOMs decide when to implement the two-person rule for nonnuclear support areas.
5.14.2. Assigning PINs. Assign a unique PIN to each individual when issuing badges. As a minimum, the PIN must be comprised of four digits. Use a random series of numbers that would be difficult for anyone to guess. Don't use a series of numbers, such as 4444, or the last four digits of the SSN. Don't list PINs and the people to whom they are assigned or allow individuals to write down or carry their PINs.
If someone forgets the PIN or the PIN is compromised, issue a new PIN. Design new systems to prevent unauthorized access to an individual's PIN.

5.15. Issuing Temporary and Visitor AECS Badges. AECS provides capabilities beyond those of the paper badge system. It can also create temporary and visitor badges. Issue these badges only for areas that use AECS.
5.15.1. Issuing Temporary Badges. Issue temporary badges to visitors who require unescorted entry and are staying at the facility for less than 90 days. (Issue visitors remaining more than 90 days a permanent badge.) Type or stamp a prominent letter "T" on the badge where a permanent badge would have a picture. Encode the badge to allow unescorted entry into the restricted area based on mission need.

NOTE: Don't use a temporary badge as a 1-day substitute for lost or forgotten badges. Replace lost or forgotten badges with visitor badges that require an escort.
5.15.2. Issuing Visitor Badges. Issue visitor badges to visitors requiring escorted entry. Type or stamp a prominent letter "V" where the picture would be on a permanent badge. Identify the SP unit of issue, installation, and a large serialized number on the AF Form 1199-1, **USAF Entry Control Credential Front Label**, and AF Form 1199-2, **USAF Entry Control Credential Pressure Sensitive Label**, portions of the badge. Don't place personal information on the badge or encode the badge to allow unescorted entry. You may encode badges to track the visitor's movements within the area.
5.15.3. One-Time Entry. For visitors requiring a one-time short duration visit (usually 1 day or less) follow escorted entry procedures in paragraph 5.12.

5.16. Alarm Annunciation. Annunciate alarms generated by AECS at locations staffed continuously during hours of use. Announce intruders through systems controlled by SP at locations staffed by personnel who monitor area alarms. Require remote annunciation for AECS at areas supporting nuclear resources. Require the following alarms to announce possible attempts to circumvent or bypass AECS:
5.16.1. Three failed attempts to gain entry.
5.16.2. Tailgating (two people passing through at one time [level III only]).
5.16.3. Duress alarms using prearranged duress PIN.
5.16.4. Weight-check failure (level III only).

Chapter 6

SECURITY PERSONNEL, SUPPORTING FORCES, AND SECURITY EQUIPMENT

6.1. Overview. This outlines the minimum qualifications for providing training, weapons, vehicles, and communications to security force personnel and supporting forces.

6.2. Security Force Qualifications. Airman classification program directives detail the career prerequisites for security forces. Resource augmentation duty program directives detail prerequisites for resource augmentation duty augmenters.

6.3. Security Force and Supporting Force Composition. Security forces are the foundation of the Air Force Physical Security Program. When USAF personnel from other career fields join the security force, they become supporting security force members. Under certain conditions outlined in this chapter, the security force may also comprise Air Force-DoD civilian police (US citizens), non-US national USAF employees, contract guards, other US military services and/or friendly nation military forces.

6.3.1. THREATCONs and Contingencies.

6.3.1.1. During THREATCONs and contingencies, and where country-to-country support agreements exist, non-US national USAF employees as well as friendly nation military forces may perform security roles outside of restricted areas.

6.3.1.2. During normal and contingency operations, use AF-DoD civilian police (US citizens), contractor guards, and other US military services to secure priority resources.

6.3.1.3. If a non-US national normally works in a security support position, train a USAF member to perform the function in an emergency.

6.4. Response Force (RF) Requirements. Response forces are required in support of AF restricted areas. They provide a capability, relative to the security priority of the resource protected, to respond and neutralize threats. In additional to those forces required for internal restricted area security, a Security Response Team (SRT) is required at all bases supporting priority resources. See AFI 31-101 Volume 2, paragraph 3, and DoD 5210.41-M.

6.4.1. Response Force. See AFI 31-101 Volume 2, paragraph 3, and DoD 5210.41-M.

6.4.2. Backup Force. See AFI 31-101 Volume 2, paragraph 3, and DoD 5210.41-M.

6.4.3. Augmentation Force. See AFI 31-101 Volume 2, paragraph 3, and DoD 5210.41-M.

6.5. Supporting Force Composition. Supporting forces include:

6.5.1. Every AF member assigned to an installation with priority resources.

6.5.2. DoD civilians or contractors who may enter restricted areas unescorted.

6.5.3. All personnel who work in restricted areas. These people provide support by applying internal controls and, in some cases, by providing armed support.

6.6. Security Force Responsibilities.

6.6.1. Shift Leaders. Shift leaders oversee supervision of each shift.

6.6.2. Shift Sergeants. Shift Sergeants:

6.6.2.1. Manage the basic operative and administrative functions of the shift.

6.6.2.2. Assume the duties of absent shift leaders or serve as leaders if none is authorized.

6.6.3. Squad Leaders. Squad Leaders directly supervise and train:

6.6.3.1. Fire team (FT) leaders.

6.6.3.2. Squad specialists such as ECs and security controllers.

6.6.4. Area Supervisors. Area Supervisors serve as senior security force members assigned to specific restricted areas.

6.6.5. Entry Controllers (ECs). ECs control entry to restricted areas.

6.6.6. Assistant Entry Controllers:

6.6.6.1. Search vehicles and personnel.

6.6.6.2. Help the EC at a restricted areas containing nuclear resources.

6.6.7. Close Boundary Sentries (CBSs). CBSs are posted to provide security surveillance over the boundary of the restricted area and/or the resources in a restricted area. This measure is normally performed by IDS.

6.6.8. Close-in Sentries (CIS). CISs control entry and guard nuclear resources or aircraft designated priority “A”. They are posted at and are normally restricted to the immediate area containing the resource. This measure can also be performed by IDS.

6.6.9. Immediate Visual Assessment (IVA) Sentries. IVA sentries provide surveillance over IDS sectors or zones when CCTV systems fail or when the MSCFO can’t see because of poor visibility or blind zones.

6.6.10. Master Surveillance Control Facility Operators (MSCFOs). MSCFOs:

6.6.10.1. Operate IDS used to secure priority resources in restricted areas.

6.6.10.2. Assess exterior IDS by line-of-sight or using closed-circuit television (CCTV).

6.6.10.3. Control entry into structures, alert shelters, and individual resources protected with IDS.

6.6.10.4. Act as a subordinate control center for security forces posted during normal operations.

6.6.11. Security Response Teams (SRTs). SRTs are external units consisting of 2 security force members who can tactically respond within 5 minutes to priority resource emergencies.
6.6.12. Alarm Response Team (ARTs). ARTs are internal area units consisting of 2 security force members dedicated to a restricted area to respond immediately if possible, but no longer than 5 minutes, to alarms or incidents. Two-person ARTs may work as two, single-person mobile patrols.
6.6.13. Alarm Monitors. Alarm monitors control entry into alarmed storage structures, alert aircraft shelters and other facilities protected by IDS.
6.6.14. Security Controllers. Security controllers direct security forces during normal and emergency security operations.
6.6.15. Alert Fire Team (AFTs). AFTs consist of 4 security force members dedicated to nuclear resources. Until dispatched, at least one of the AFTs must remain in hardened AFT facilities provided within their assigned restricted areas.
6.6.16. Mobile Patrols. Mobile patrols consist of a security force member dedicated to a specific restricted area or individual resource. The mobile patrol must watch over assigned resources and respond to alarms and incidents.
6.6.17. Mobile Fire Teams (MFTs). MFTs consist of 4 security force members on a FT or any combination of SRTs, ARTs, and mobile patrols. MFTs respond to situations involving priority resources and may work in smaller teams.
6.6.18. Remote Display Area Operator (RDAO). Remote display area operators support MSCFOs by monitoring the remote display annunciator for restricted areas containing nuclear weapons. See AFI 31-101 Volume 2, paragraph 3.

6.7. Security Force Training. Air Force training instructions outline the minimum proficiency training required for security force members. In addition to this publication, you can find more training requirements for security force members supporting nuclear weapons in DoD 5210.41-M.
6.7.1. Security force members must be thoroughly familiar with the use-of-force rules and local theater-unique requirements.
6.7.2. Commanders must implement an initial and recurring physical security awareness program.

6.8. Arming Security Forces. Security forces are armed as shown below. AFC 21-209, *Ground Munitions,* specifies ammunition quantities for security forces. MAJCOMS specify the fighting load for security forces supporting nonnuclear priority resources.
6.8.1. Fighting Load (FL). The munitions quantity individuals or gun crews are issued for duty, and carry on their persons or gun crews have immediately available. AFC 21-209, *Ground Munitions,* authorizes each AF installation to issue a FL to each security force member with an M16 rifle with at least half of the basic quantity of ammunition.
6.8.2. Basic Quantity (BQ). The munitions quantity authorized to establish a stockpile from which to issue FLs to persons and gun crews performing armed duties.

6.9. MAJCOM Determinations. MAJCOMs may specify the FL or delegate responsibility to ISCs to determine the type of weapons and FL for security forces supporting nonnuclear priority resources as well as those carried by:
6.9.1. Element leaders and element sergeants who perform both law enforcement (LE) and security functions.
6.9.2. Other security posts not part of the RF and BF.
6.9.2.1. Security force members assigned to a nuclear supporting RF or BF must carry the basic quantity, as outlined in AFC 21-209.
6.9.2.2. Forces which, in an emergency, engage adversaries in the open, must carry M16s.
6.9.2.3. Entry controllers who work in restricted areas containing nuclear weapons may carry a handgun but must have an M16 readily available.
6.9.3. Additional RF Requirements. Security force planners equip the RF elements supporting nuclear weapons with:
6.9.3.1. Grenade Launchers.
6.9.3.1.1. One per on base ART & SRT, all nuclear supporting FTs. MAJCOMs should consider arming ARTs & SRTs supporting missile field operations with grenade launcher.
6.9.3.1.2. Four for each BF.
6.9.3.2. Machine Guns.
6.9.3.2.1. M60s for each permanent nuclear weapons storage and nuclear generation area. Give the first to an AFT; the second to other elements of the RF for support.
6.9.3.2.2. M60s for the BF. Give one to each missile field FT, missile ground convoy lead and trail FT, and missile ground convoy airborne FT. If you don't use airborne support, add a ground FT and equip it with one M60.
6.9.3.2.3. M60s for securing areas with nuclear-loaded logistics aircraft.
6.9.3.3. Grenade Machine Guns (MK19). MAJCOMs that prescribe the MK19 must arm the assistant with an M16 and the gunner with a sidearm.
6.9.3.4. Other Equipment. All security force members must have gas masks, body armor, and helmets available for immediate use.

6.9.3.4.1. Select body armor most appropriate for your command using the National Institute of Justice (NIJ) Consumer Product List (CPL) as a guide. The NIJ Technology Assessment Program lists body armor models in their CPL that have been tested by the NIJ and found to comply with the requirements of *Ballistic Resistance of Police Body Armor: NIJ Standard-0101.03 (April 1987)*. Armor that complies with this standard meets the minimum performance requirements critical for police protection.

6.9.3.4.2. Generally, type II-A body armor, which is sufficiently comfortable for full-time wear, protects against .357 Magnum velocity weapons. Type III-A, which provides the highest level of protection (to include 7.62 mm) is considered to be unsuitable for routine wear. This armor is appropriate for use in high threat areas.

6.9.3.4.3. It's not necessary to replace serviceable flak vests with body armor unless warranted by a specific threat. Replace unserviceable flak vests with body armor through attrition.

6.9.4. Arming Requirements for Support Personnel. MAJCOMs prescribe support personnel arming requirements. In nuclear weapons storage areas, provide at least enough firearms and ammunition (half the basic quantity) to arm all military personnel assigned to the area on a normal duty shift.

6.9.5. Hand Grenades.

6.9.5.1. Nuclear security forces must carry at least six riot or burning hand grenades, from either of these two types:

6.9.5.1.1. M25A2, Riot, Bursting Type, National Stock Number (NSN) 1330-00-645-6211 G924.

6.9.5.1.2. M7A3 Burning Type NSN 1330-00-965-0802-G963.

6.9.5.2. All nuclear supporting RFs must carry at least four smoke grenades (NSN 1300-00-219-8511G930).

6.10. Security Force Vehicles. ARTs, SRTs, FTs, element leaders, element sergeants, area supervisors, and mobile patrols require appropriate vehicles. All permanently assigned security force vehicles must have emergency lights, sirens, and a public address system.

6.10.1. Commanders provide armored vehicles to:

6.10.1.1. AFTs.

6.10.1.2. The lead and trail vehicles for off-base convoys within the continental United States (CONUS).

6.10.1.3. The lead and trail convoy security teams for on- and off-base convoys outside of continental United States (OCONUS).

6.10.2. Additional Armored Vehicle Applications. In consideration of the threat, the size of the response area, topography, and security force tactics, MAJCOM and local security planners should assign armored vehicles to the following security force elements:

6.10.2.1. Other FTs supporting convoys.

6.10.2.2. Missile security MFTs and SRTs.

6.10.2.3. Back-up force FTs.

6.11. Security Force Communications. Units must make the best possible use of systems which provide secure voice capabilities or comply with data encryption standards. As existing non-DES systems reach the end of their life cycles, units must incorporate DES into replacement systems.

Provide land-mobile radios, base stations, and/or repeaters with an uninterruptible power source.

6.11.1. Security Force Radio Net Capabilities. Installations supporting priority resources must have a security force radio net with at least two frequencies or the system must allow the security force continuos communications during radio net saturation, jamming, or interference conditions. Nuclear units must comply with DoD 5210.41M, chapter 5, section 6. You must assign and issue radio frequency authorizations according to AF frequency authorization directives.

6.11.2. Radio Equipment Distribution. Security force planners:

6.11.2.1. Give each static security force member a portable or fixed radio. Give FTs one radio per two people.

6.11.2.2. Equip each vehicle regularly used by the security force with a mobile or portable-mobile radio.

6.11.2.3. At each installation with priority resources, back up the land mobile radio (LMR) system with a land-line system.

6.11.2.4. Install direct/hot-line instruments at each permanent static post.

6.11.2.5. Ensure that units devise manual systems at each installation with priority resources to back up the LMR and land-line systems.

Chapter 7

PHYSICAL SECURITY PROGRAM FACILITIES

7.1. Overview. This describes the facilities and associated equipment supporting the physical security program. You must apply these criteria to all upgrades of existing facilities and equipment, as well as all new equipment and facilities.

7.2. Support Facility Requirements.

7.2.1. Central Security Control (CSC). Each nuclear support installation must establish a primary CSC to provide C3 for the on-duty security force. Central Security Control (CSC). Each nuclear support installation must establish a primary CSC to provide C3 for the on-duty security force.

NOTE: At installations possessing only priority B and C and nonnuclear priority A resources, the local ISC may designate the law enforcement desk (LED) as the CSC.

7.2.1.1. Designate a windowless security force C3 room as a controlled area for CSC. The room must have:

7.2.1.2. Suitable ventilation, heating or air conditioning.

7.2.1.3. Doors that lock when not in use and a cipher lock or level 1 AECS on the main entry door. (See Paragraphs 5.13 through 5.16 for information on AECS.)

7.2.1.4. A one-way glass panel or similar viewing device set in the main door to identify people requesting entry who don't have the cipher code.

7.2.1.5. An auxiliary power unit or alternate source of electrical power (independent of the normal base power system) for operating essential lights, communication, and alarm equipment during emergencies.

7.2.1.6. Alarm system annunciator panels and remote annunciator displays for the IDS.

7.2.1.7. The main terminal for the LMR base station and land-line system.

7.2.1.8. Direct line communications between the security force controller and the person(s) at the CSC entrance requesting entry. Also provide land-line communication with each fixed, permanent, static sentry post, command post, control tower, LED, fire department, subordinate C3 facilities, flight line job control, and munitions control.

7.2.1.9. Support rooms, including an office for the on-duty element leader and element sergeant, security force break room and a covered area or room for guard mount.

7.2.2. Alternate CSC. Equip an alternate CSC to serve as C3 back-up for the security force. Installations:

7.2.2.1. Maintain uninterrupted alternate C3 from a fixed location, manned 24-hours-a-day for units supporting nuclear resources.

7.2.2.2. Equip a mobile unit, a manned post, a subordinate C3 center, or LED to provide uninterrupted C3 during transitions between the primary and alternate CSC locations if the alternate isn't housed at a continuously staffed facility.

7.2.2.3. Activate the alternate CSC with a dedicated security force controller during increased threat periods.

7.2.2.4. Equip the alternate CSC with an auxiliary electrical power supply.

7.2.2.5. Maintain an alternate 24-hours-a-day C3 capability at nonnuclear support units. Use a fixed or mobile alternate C3. If fixed, equip it with two-way radio communications (preferably a base station) and direct or dial land-line backup to all facilities listed in paragraph 7.2.1.

7.2.3. Master Surveillance Control Facilities (MSCF). Installations needing IVA of exterior IDS alarms include an MSCF (tower or ground level) as part of their security systems. Security force planners must ensure MSCFs:

7.2.3.1. Are small-arms hardened and operate inside the restricted area when they support nuclear resources.

7.2.3.2. Have land-line and LMR equipment to allow MSCFOs to control entry into structures, shelters, or individual resources in the area and communicate with on-duty security forces.

7.2.3.3. Have primary lighting controls for area and boundary lighting, a base station radio, and a public address system.

7.2.3.4. MAJCOM and base planners should consider the cost of alarm monitoring and assessment, and survivability tradeoffs of elevated towers versus ground/below ground MSCFs.

7.2.4. Alert Fire-Team Facilities. Installations must have an alert FT facility in all permanent restricted areas containing nuclear resourcesAlert Fire-Team Facilities. Installations must have an alert FT facility in all permanent restricted areas containing nuclear resources. **EXCEPTION:** Deployed missile and weapon storage and security system (WS3) areas, as defined in DoD 5210.41-M. In regard to alert FT facility garage doors, the obscuration provided by a solid garage door satisfies the hardening requirement contained in DoD 5210.41M.

7.2.5. Entry Control Facilities (ECF). Use the guidelines in DoD 5210.41-M to design and construct ECFs for permanent restricted areas containing nuclear resources. **EXCEPTION:** Deployed missile and WS3 areas. Security force planners must ensure that ECFs:

7.2.5.1. Provide land-line communication for people requesting entry to the area.
7.2.5.2. Shelter the EC from the elements by equipping them with heating or air-conditioning, light, ventilation, and direct land-line communication to CSC.
7.2.5.3. If not small-arms hardened, protect the ECs from small-arms fire with, hasty fighting positions, barriers, body armor, or other means.
7.2.6. Sentry Shelters. All normal security fixed posts must have sentry shelters equipped with heat, light, and ventilation. Local security force leaders decide whether to small-arms harden the shelters or protect sentries through other means. Fighting positions used for permanent restricted areas supporting nuclear resources must meet the requirements of DoD 5210.41-M.
7.2.7. Security Force Armory. Store security force weapons, ammunition, and equipment in a room or facility that meets the requirements in AFI 31-209, *Air Force Resource Protection Program.*
7.2.8. Alternate Arming Point. Installations that support nuclear resources and ISC-designated installations, must store enough weapons and ammunition at a separate location to equip at least the BF.

7.3. Boundary Barriers. Boundary barriers mark the legal and physical boundaries of a restricted area and notify intruders you will use deadly force, if necessary, to stop them. The physical security program uses boundary barriers ranging from painted red lines to dual chain-link fences. Planners find barrier requirements in AFH 32-1064, *Standard Facility Handbook*

7.4. Barriers for Permanent Restricted Areas Containing Nuclear Weapons. (See DoD 5210.41-M.)
7.4.1. Fabric. Installations must use woven 9-gauge (.1483 inches or 3.7 mm), steel-wire, chain-link fabric for type A fencing, with 2-inch (5.1 cm) square mesh. Steel-wire fabric must have a steel core that measures 9 gauge, not including the coating. **EXCEPTION:** At North Atlantic Treaty Organization (NATO) sites, the Supreme Headquarters Allied Powers Europe criteria for steel fabric apply.

NOTE: Coated steel wire purchased or installed before 1 January 1980 meets the 9-gauge steel core requirement as long as the core wire is a least 11 gauge (.1205 inches or 3.1 mm).
7.4.1.1. Use non-reflective paint for fences to reduce glare affecting assessment.
7.4.2. Mountings. Installations:
7.4.2.1. Mount fence fabric on metal posts of appropriate height set in concrete with additional bracing at corners and gate openings, as necessary.
7.4.2.2. Use reinforced-concrete posts if metal posts are not available.
7.4.2.3. Put posts, bracing, and other structural members on the inside (site side) of the fence fabric.
7.4.3. Height. The aboveground height of the mesh fabric must measure
7 feet (approximately 2.13 m).
7.4.4. Topping. Installations:
7.4.4.1. Install two 15-inch outriggers, each having three stands of barbed wire, at intervals along the top of the fence.
7.4.4.2. Install the outriggers at 45-degree angles in a "Y" configuration.
7.4.4.3. Units may install a type of barbed tape or concertina roll between the "Y" outriggers.
7.4.4.4. Secure the topping tape to every post and no less than every 18 inches along the fence fabric to the top rail reinforcing wire or barbed-wire strand.
7.4.4.5. Units may use fences installed with single vertical arm taut wire sensor systems on top of a fence instead of standard 15-inch, three-strand, barbed-wire outriggers.
7.4.4.6. Install a top rail or taut reinforcing wire at the top of the fence to stabilize the fence fabric.
7.4.5. Anchoring and Stabilizing.
7.4.5.1. Installations must extend the bottom of the fence fabric to within
2 inches (5 cm) of firm ground and anchor it to prevent intruders from lifting the fabric and creating an opening more than 5 inches (12.5 cm) in height. To do this, use horizontal bottom rails, concrete curbs or sills, sheet piling, piping, or other inexpensive materials.
7.4.5.2. Stabilize surfaces in areas where loose sand, shifting soils, or surface waters cause erosion and that could allow an intruder to penetrate the perimeter security system. Where you can't stabilize the surface, provide concrete curbs, sills, or other similar types of anchoring devices and extend them below ground level.
7.4.5.3. Secure the fence fabric to fence posts, rails, or other anchoring material with fasteners of tensile strength at least equal to that of the fence fabric. Firmly secure fence fabric to tension wires with 12-gauge galvanized tie wire incorporating at least a 540-degree tightened loop.
7.4.6. Gates. The gate fabric or support must reach to within 5 inches of paved surfaces and to within 2 inches of other surfaces. It must prevent someone from lifting the fabric to create an opening more than 5 inches high. The maximum allowable distance between the gate posts and gate is 5 inches when the gate is closed.

7.4.6.1. Gates must be closed and locked when not in use. Gates are considered locked when they are equipped with an electric opening or closing device that, when closed, prevents the gate from being opened by hand.

NOTE: During power outages, the lock must "fail" in the locked position.
7.4.6.2. Use a type II or III secondary padlock on manually operated gates that don't have an electric lock. Secure the key at the ECF.
7.4.6.3. Don't open both pedestrian or both vehicle gates at the same time unless an armed security force member is posted between the open gates.
7.4.7. Elevated Barriers. When possible, use elevated barriers (such as rope, chain, or tape) rather than painted red lines. If you must use painted lines, for example, for taxiway gaps, use a wide-painted line in a bright color, such as red-orange, fluorescent, or other reflective color.

7.5. Barriers for Restricted Areas Containing Nonnuclear Resources. Type A fencing (see Paragraph 7.4) is required for all restricted areas. Installations may use existing fencing kept in a good state of repair. Install type A fencing when replacing or creating new restricted area boundaries.
7.5.1. Other Barrier Requirements for Nonnuclear Resources.
7.5.1.1. In cases where terrain, soil, surface waters, and other environmental factors make it impossible to meet type A anchoring and stabilization criteria, installations need not request a formal deviation. Document the deficiencies and compensatory measures in appropriate security force instructions.
7.5.1.2. During installation, stabilize fencing that also serves as a sensor system platform to meet sensor siting requirements.
7.5.1.3. When possible, use elevated barriers (such as rope, chain, or tape) rather than painted red lines. If you must use painted lines, for example, for taxiway gaps, use a wide-painted line in a bright color, such as red-orange, fluorescent, or other reflective color.

7.6. Clear Zones. Create a clear zone for permanent restricted areas that contain priority A and B resources and new areas (built after 3 October 1988) that contain priority C resources upgraded to priority A or B during contingencies.
7.6.1. Clear Zone Specifications. To create a clear zone:
7.6.1.1. Level a belt of land at least 30 feet on both sides of a single boundary barrier.
7.6.1.2. Level at least 30 feet inside the inner fence, the entire area between fences, and 30 feet outside the outer fence for dual fences.
7.6.1.3. Remove all possible dips, ridges, ditches, and objects that could conceal an intruder or obstruct vision from permanent restricted area clear zones.
7.6.1.4. Position poles (lighting, power, camera, etc.), overhead wires, and other features so they can't circumvent the sensor system or fence.
7.6.1.5. MAJCOMs specify clear zone requirements for restricted areas with priority C resources that aren't upgraded.
7.6.2. Vegetation Control.
7.6.2.1. For permanent restricted areas containing nuclear resources, limit underbrush in the area, in the clear zones, and between the fences to 8 inches.
7.6.2.2. For other restricted areas, MAJCOMS determine the height of underbrush so that it can't conceal an intruder.
7.6.2.3. Trim or prune vegetation to avoid removing plants preventing ground erosion and to avoid cutting down protected plants.

7.7. Facility Spacing. Locate the boundary barrier for restricted areas containing Priority A resources at least 250 feet from the base perimeter or property line. If the restricted area boundary is closer than 250 feet to the base perimeter or property line, allow 100 feet between the boundary barrier and the resources. Locate area boundary barriers (if you are building a double fence, the inner fence) at least 50 feet from the resources you are securing. **EXCEPTION:** Deployed missile facilities or WS3 areas.

7.8. Lighting Requirements for Restricted Areas Containing Nuclear Weapons. Permanent areas containing nuclear weapons require boundary, area, and entry-point lighting. For more information, see paragraphs 7.8.1 through 7.8.4 and DoD 5210.41-M.
7.8.1. Boundary Lighting. Use different lighting levels depending on the mode of IVA. For design and initial construction acceptance of boundary lighting, use .2 foot candles for human IVA and 2.0 foot candles for CCTV IVA of alarms in the assessment zone. Thereafter use the lighting ratios in paragraphs 7.8.1.2. for visible-light systems and 7.8.2.1 for non-visible light systems, to measure lighting standards. The boundary system must provide the lighting level required for IVA.
7.8.1.1. Use boundary lighting circuits designed to ensure that failure of one or more lights doesn't affect the remaining lights.

7.8.1.2. CCTV assessment may use visible-, or low-, or no-light systems. Establish foot candle levels which will ensure adequate assessment. Set the maximum-to-minimum light level ratio at less than 6:1; and the average-to-minimum light level ratio at less than 3:1. Measure these ratios in each CCTV zone of coverage by observing the TV monitor and determine where the darkest and lightest positions are located in the zone. Take light measurements at those locations and calculate the light to dark ratio from those readings.

NOTE: These ratios apply only to assessment zones using CCTV.

7.8.1.3. Make sure that the visible lighting systems for CCTV and human IVA have an instant restart capability and achieve the required lumen output as quickly as technology allows but in no more than 65 seconds after losing prime power.

7.8.1.4. Install lighting controls in the MSCF and ECF. The MSCF controls must override those in the ECF in emergencies.

7.8.1.5. Locate all fixtures, wiring, switches, and transformers inside the restricted area. For new or modified construction, install light poles at least 24 inches from the inner boundary fence with luminaries no higher than 35 feet. Position poles (lighting and camera) and fixtures so they can't be used to circumvent the sensor system and the fence. Distribute power underground when possible.

7.8.2. Very Near Infrared (VNIR) Lighting Systems. VNIR systems must provide a minimum illumination of 5 microwatts per square centimeter in the band from .8 to 1.1 microns, measured horizontally 6 inches from the ground.

7.8.2.1. Set the maximum-to-minimum light ratio at less than 6:1. Measure these ratios using the procedure described in paragraph 7.8.1.2.

7.8.2.2. In less than 1/2 second after being switched on, VNIR luminaries must achieve at least 90 percent of rated power output.

7.8.2.3. For VNIR CCTV assessment systems, VNIR luminary switchings must be tied to the alarm system in a manner to assure immediate assessment capability.

7.8.2.4. Equip low- or no-light systems with a visible-light capability that the RF can use in emergencies.

7.8.3. Area Lighting. Use area lighting to illuminate the interior of the restricted area to help personnel detect and track intruders. Switch lighting by sectors to avoid unnecessary illumination and maximize the security-force advantage. Area Lighting. Use area lighting to illuminate the interior of the restricted area to help personnel detect and track intruders. Switch lighting by sectors to avoid unnecessary illumination and maximize the security-force advantage. **EXCEPTION:** Because of the large size of Nellis and Barksdale AFB weapons storage areas, it is not necessary to illuminate the entire interior of the areas. Illuminate the areas surrounding the near vicinity of storage structures and maintenance and inspection facilities. The exact distance lighting must extend around these facilities is not specified. However, it must be adequate to support the security force's planned tactical defense of these areas.

7.8.3.1. Locate lighting controls, including those on structures or shelters when they make up part of the area lighting system, in the MSCF and the ECF.

7.8.3.2. Give the MSCF override capabilities.

7.8.3.3. Locate all fixtures, wiring switches, and transformers inside the restricted area. When possible, distribute power underground or encase them in hardened conduit.

7.8.3.4. Provide an alternate power source.

7.8.3.5. Sectorize the lighting to avoid unnecessary illumination of the entire area and to maximize the security-force advantage.

7.8.3.6. As a goal the lighting should provide an average intensity of at least 0.2 foot candle measured vertically, 6 inches above the ground, throughout the area.

7.8.4. Entry-Point Lighting. Use entry-point lighting at all permanent restricted areas. **EXCEPTION:** Deployed missile facilities.

7.8.4.1. Install a lighting system at the EC's position that provides shadow-free light, when possible, and clearly illuminates the entrant's:

7.8.4.1.1. Physical appearance.

7.8.4.1.2. Clothing.

7.8.4.1.3. Hand-carried objects.

7.8.4.1.4. Face.

7.8.4.2. Provide battery-sustained emergency lighting and portable lights or flashlights to support entry-control functions if the primary and alternate power sources fail.

7.9. Lighting Requirements for Permanent Restricted Areas Containing Nonnuclear Priority Resources.

7.9.1. Boundary Lighting. When restricted areas are fenced and the security system is designed to detect intruders at the boundary, install boundary lighting that meets the criteria outlined in paragraph 7.8.1. and 7.8.1.2. or 7.8.2.1. When the security system doesn't include an MSCF, install the lighting controls inside the ECF.

7.9.2. Area Lighting. Installations must provide sufficient lighting to detect intruders before they reach and damage protected resources. See MAJCOM guidelines for the area lighting concept.
7.9.3. Entry-Point Lighting. Provide entry-point lighting at all entry points protected by security forces. Provide entry-point lighting for priority A and B resources meeting the requirements of paragraph 7.8.4.
7.9.3.1. For entry points to restricted areas containing priority B resources, provide only a secondary power source or emergency lighting such as battery-sustained emergency lights, or flashlights.
7.9.3.2. MAJCOMs routinely protecting entry points to areas containing priority C resources must outline the lighting criteria for these locations.
7.9.4. Special-Purpose Lighting. Lighting fixtures may range from hand-held spotlights to wheel-mounted floodlight sets (light-alls). Use special-purpose lighting to support any area containing priority resources during normal or contingency operations to compensate for inadequate or inoperative boundary, area, or entry-point lighting.

7.10. Detection Enhancement Devices. Certain operations may dictate a low-signature environment. MAJCOMs must outline deployment procedures for using such devices, including thermal-imagery and night-observation devices.

7.11. Warning Signs. Display restricted area signs along the restricted- area boundary at 100-foot intervals. Make sure that intruders can't climb them.
7.11.1. Warning Sign Specifications.
7.11.1.1. Use AFVA 31-101, or appropriate MAJCOM visual-aid restricted area signs, mounted on metal backings. Translate signs into the host-nation language if in a foreign country or in areas where languages other than English predominate.
7.11.1.2. Use accepted danger or warning symbols on signs in areas with widespread illiteracy. Use white for the sign's background. Paint the words "WARNING" and "USE OF DEADLY FORCE AUTHORIZED" in red and the remaining words in AF blue or black.
7.11.1.3. If military working dogs support the area, post AFVA 125-13, *Military Working Dog Notice*, directly below AFVA31-101. Obtain MAJCOM approval before posting AFVA 125-13. Requirements depend on local or country limitations. Use a white background on such signs and AF blue or black for the lettering.
7.11.1.4. Use existing signs that differ in size or color if the wording meets AFVA requirements or can be corrected. When you replace them, match AFVA 31-101 size and color requirements.
7.11.1.5. The AF encourages the use of reflective surfaces.
7.11.1.6. Don't place warning signs on fences with IDS.
7.11.1.7. Construct signs directing the removal of ignition keys from parked vehicles. Place these signs next to and inside restricted areas containing nuclear weapons.

7.12. Locks and Hasps. When securing structures or shelters containing priority resources, use locks and hasps compatible with the facility to which they are attached.
7.12.1. Specifications for Locks and Hasps.
7.12.1.1. High security padlocks must conform to military (MIL) specification MIL-P-43607.
7.12.1.2. Secondary padlocks must meet the requirements of commercial item description (CID) A-A-1927C and MIL standards (STDs) 21313G, *Pad Lock Sets - Individually Keyed and Keyed Alike*, 10 Jul 92, and 35647E, *Pad Lock, Key Operated*, 29 Jul 92. Use one of three types of secondary padlocks:
7.12.1.2.1. Type I, which consist of a hardened steel shackle with a case of steel, malleable iron, or die cast zinc alloy.
7.12.1.2.2. Type II, which have a hardened steel shackle and brass or bronze case.
7.12.1.2.3. Type III, which have a brass or bronze shackle and case.

7.13. Locking Nuclear Weapons Storage Structures or Alert Aircraft Shelters. See DoD 5210.41-M.
7.13.1. Sliding Bolts. On doors that require a single sliding bolt, use a solid steel rod or bar (cold rolled steel) not less than 1 inch in diameter. On doors that require two sliding bolts, use a solid rod or bar (cold rolled steel) not less than 1/2 inch in diameter. For all sliding bolts, the receiving hole made in the wall, door frame, or floor must not measure less than 3 inches deep.
7.13.2. Installation. For installation procedures, see AF T.O.s (44 H2 series (*Installation of Security Hardware*)) and *Guidelines for Application of Security Hardware Relating to Bunkers, Igloos, Huts, and Other Enclosures,* Jun 74, by ST Athas. Order this publication from the US Army Natick Laboratories, Natick MA 01760.
7.13.3. Key Accountability. Installations must not hold security forces responsible for safeguarding and issuing storage structure keys. However, when no supporting forces work within weapons storage areas, maintenance and assembly building keys may be kept at the ECF. Set up formal accountability controls in accordance with AFI 21-204, *Nuclear Weapons Procedures,* to ensure that only authorized personnel receive these keys.

7.13.4. Nonnuclear Resource Security. Locks (with compatible hasps), used to secure other than nuclear resources must meet requirements for secondary padlocks in CID A-A-1927C and MIL-STD 21313G and 35647E.

7.14. Alternate Power Supplies. (See DoD 5210.41-M for nuclear support requirements.) In nuclear areas, all command and control centers must install switches that automatically change systems to an alternate power source. The AF recommends automatic switching to alternate power for all nonnuclear restricted areas.

NOTE: Don't apply for a deviation if you have programmed but haven't installed this capability in nonnuclear areas. Make sure security forces can manually start alternate power equipment.

7.14.1. Specifications for Alternate Power Supplies.

7.14.1.1. Protect priority A (nonnuclear) electrical power supply components on the load side of the alternate power supply from small arms fire.

7.14.1.2. Bury electrical transmission lines at least 24 inches below the ground or encase them in hardened conduit.

7.15. Grills, Grates, and Other Openings. See MAJCOM guidelines for nonnuclear restricted areas. In addition to the requirements in DoD 5210.41-M for nuclear areas, meet the following requirements:

7.15.1. Use type I or II secondary padlocks (see paragraph 7.12) with compatible hasps on openings secured by removable bars or grills, according to CID A-A-1927C and MIL-STD 21313G and 35647E. When securing manhole covers, use of a uniquely keyed, flush mounted, locking bolt is acceptable in lieu of a Type I or II lock.

7.15.2. Use any type secondary padlock or non-locking devices with seals for openings that security forces frequently observe over the course of a day. MAJCOMS approve non-locking devices which provide the equivalent delay of the specified padlocks and hasps.

7.15.3. Secure openings both inside and outside of the restricted area.

7.15.4. Conduct random inspections of all unsensored openings each shift.

7.15.5. New and upgraded boundary sensor systems should include coverage of boundary openings.

7.16. Daily Checks. Each on-duty supervisor for restricted areas containing priority resources must visually check all the physical security facilities, including boundary barrier systems, gates, and structures, daily for tampering, deterioration, and inoperative equipment. Owning and using personnel check areas when security forces aren't assigned.

7.16.1. Nuclear Weapons Storage Structure Checks. Inspect the exterior of all structures containing nuclear weapons at least every 4 hours during munitions-maintenance non-duty hours for signs of tampering and covert entry. Record your observations.

7.16.2. Joint End-of-Day Checks.

7.16.2.1. Before munitions-maintenance personnel leave the weapons storage area, they visually inspect and test area and maintenance-assembly-building locks with the area security supervisor and a munitions-maintenance supervisor. **EXCEPTION:** At nuclear munitions squadrons, an ART accompanied by a maintenance representative may check these areas.

7.16.2.2. The area supervisor ensures personnel complete the checks and record their observations in the SP blotter or other suitable form.

7.16.3. Lighting Checks. Conduct visual surveys of perimeter, area, and special purpose lighting when such lighting is activated during normal area operations. Record results and request repair as necessary. At least weekly, conduct a complete lighting inspection of all lighting to ensure operability. This inspection may be completed incrementally throughout the week. Owning and using personnel check area when security forces aren't assigned.

Chapter 8

INTRUSION DETECTION SYSTEMS (IDS)

8.1. Overview. The term IDS is used singularly when referring to an individual intrusion detection system and in plural when referring to general IDS requirements. This chapter describes specific IDS requirements for

the boundaries of permanent restricted areas containing priority A, B, and C resources; facilities containing these resources; the resources themselves; and testing and maintaining IDS and components.

8.1.1. Planning. Don't replace electronic security components purchased or installed before 1 Oct 1994 only to meet this instruction's standards. Upgrade when components deteriorate (normally in 10 years for interior sensors and 5 years for

exterior sensors). MAJCOMS must develop a pre-planned product improvement and replacement program to ensure long-term IDS support.

8.1.2. Programming. The Air Force Base and Installation Security Systems (BISS) program directs the procurement, installation, deployment, and logistics support of Air Force IDS. Within the BISS program: 8.1.2.1.

HQ AFMC-ESC manages IDS procurement and logistics consistent with established priorities and funding.

8.1.2.1. Operating Commands define specific requirements, program for installation of new systems, and ensure BISS program funds are adequate to facilitate system life cycles and upgrades as necessary.

8.1.2.2. Operating Commands may do this by directly funding their needs in the BISS program or by influencing the BISS sustainment program element (PE) in the Air Force Program Objective Memorandum.

8.2. General Description. IDS comprise a mix of equipment and components. Components may include exterior sensor equipment; structure and shelter sensor equipment (entrance and interior); individual resource sensor equipment; integrated AECS; alarm data transmission equipment; assessment equipment; and alarm annunciation and display equipment.

8.2.1. Concept. Security forces must understand the strengths and weaknesses of sensor systems. All sensor pheomenologies have weaknesses that may be exploited. For example, boundary IDS primarily detect the unskilled or semiskilled intruder. It doesn't adequately detect the skilled or highly skilled threat. For this reason, security planners must use boundary sensor equipment as a component of the overall restricted area security system. Create a complex security environment including active patrolling; physical obstacles to intrusion, such as fences, locks, and structure delay mechanisms; sensors; security lighting; and posted sentries.

8.2.2. Units operating IDS must document the technical capabilities of the components employed and show how other elements of the security system offset IDS limitations.

8.3. Selecting IDS and Components.

8.3.1. Considerations. When selecting IDS or components, consider the adequacy of maintenance and operator training; the adequacy of T.O.s and maintenance support; complementing sensor phenomenologies; compatibility with previously installed equipment; and known probability of detection (Pd) and invalid alarm rates (IAR).

8.3.2. IDS Approval. HQ USAF/SP must approve systems and components used in restricted areas for detecting intruders, assessing intrusions, displaying intrusions electronically, transmitting data, controlling entry, and delaying and denying entry.

8.3.2.1. Base approval on review of Air Force developmental test and evaluation (DT&E) and operational test and evaluation (OT&E) data. Tests not conducted by the Air Force Operational Test and Evaluation Center (AFOTEC) may be considered for approval of IDS. However, this data must clearly indicate the supporting test(s) provided an equivalent level of quality, control, objectivity, and validity as that provided by an AFOTEC test

8.3.2.2. Program Management. HQ AFSPA monitors the development process of AF IDS requirements. They monitor tests and assess the data submitted by all test agencies. Additionally, this office obtains the recommendations for approval or disapproval from these agencies and assesses all recommendations provided. HQ AFSPA forwards recommendations and rationale to HQ USAF/SP.

8.3.2.3. HQ USAF/SP approves systems or components when the test data shows their effectiveness in the tested applications and configurations. Different applications or configurations may require additional testing and approval. HQ AFSPA recommends and HQ AF/SP periodically publishes and updates a listing of approved IDS. The listed IDS may be used in nuclear and nonnuclear applications provided testing is completed as outlined in paragraph 8.3.2.1.

8.3.3. IDS as Enhancements. MAJCOMs choosing to procure unapproved IDS to enhance existing physical security must provide support for maintenance, logistics, and training.

8.3.3.1. MAJCOMs may not rely on unapproved IDS enhancements to deviate from existing physical security policy.

8.4. Detection Requirements. Each intrusion detection system for exterior areas, structures, shelters, or individual resources involving priority resources, consists of one or more levels of alarm and/or one or more lines of detection using IDS sensors.

8.4.1. Line of Detection. IDS equipment, regardless of type, must detect all reasonable intrusion scenarios, including surreptitious attempts to spoof, tamper or bypass the detection line(s). A line of detection, using a restricted area fence as the sensor platform, must detect cutting, climbing on, or lifting the fence fabric. A line of detection at the area perimeter, in a clear zone, at a taxi way gap, or around exposed individual resources, must detect walking, running, rolling, crawling across, or jumping through the line of detection. A line of detection at a structure or shelter must detect intrusion attempts through the doors, walls, roof, or vents.

8.4.2. Interior IDS Coverage. Economically, total IDS coverage of the entire interior of a structure or shelter is difficult to achieve. The AF allows unsensored areas, or dead zones, in structures or shelters as long as they don't allow intruders approaching from doors, walls, roofs, or vents to reach the resource before setting off an alarm.

8.4.2.1. Substantially constructed structures and shelters, such as weapons storage area (WSA) storage structures and hardened aircraft shelters (HAS), are adequate to protect against covert penetration of floors, walls, and roofs. In structures of this type, IDS coverage must detect an intruder entering through the doors and any openings that exceed 96 square inches with the smallest dimension greater than 6.4 inches. IDS must detect intruders before they reach the resource. EXCEPTION: Structures that do not have substantially constructed roofs, such as maintenance and inspection (M&I) facilities with frangible roofs, must have IDS coverage of the roof.

8.4.3. Stay Behind Threat. IDS are often not designed to detect an authorized individual staying behind in a closed structure or shelter (after it's secured). Use supporting forces to purge the structure or shelter before securing it, to defeat this threat.

8.4.4. Level of Alarm. A level of alarm is usually only one IDS sensor. A level of alarm uses sensors to detect specific intrusions, such as running, cutting, or climbing but doesn't protect against all reasonable intrusions at a particular location. Appropriate levels of alarm are applied together to form a line of detection. In the event a single sensor becomes available that is so technologically advanced that it can detect all reasonable intrusion scenarios at a specific location, it would be considered a line of detection at that location.

8.5. Specific IDS Detection Requirements Associated with Priority A, B, and C Resources.

8.5.1. Nuclear Resources. Security police must establish two lines of detection around boundaries of permanent restricted areas containing nuclear resources. The lines of detection must support each other. For example, place each line so that an intruder can't cross the boundary, regardless of the path or method used, without defeating both lines. Based upon operational and technical assessment of the sensor types used, sensors used in one line must differ from that of the other and must be designed to offset technical limitations of the other. The planing process decreases the overall IDS vulnerability to countermeasures, environmental extremes, failure modes, and other emergencies.

8.5.2. Additional Lines. Establish an additional line of detection in structures, shelters, and individual exposed resources.

8.5.3. Probability of Detection (Pd). Lines of detection for priority A and B resources must meet a Pd of .95 at the 90 percent confidence level. Overall system Pd depends on the number of detection lines or levels of alarm applied.

8.5.4. Priority A Nonnuclear Resources. For priority A nonnuclear resources, establish one line of detection at the restricted area boundary and one line of detection at the structures, shelters, or individual exposed resources. Each line of detection must meet a Pd of .95 at the 90 percent confidence level and ensure no condition exists where a knowledgeable intruder can predict successful penetration (exploit the system) using reasonable intrusion scenarios

8.5.5. Priority B Resources. For priority B resources, establish one line of detection at the restricted area boundary plus one level of alarm at the structures, shelters, or individually exposed resources. The line of detection must meet a Pd of .95 at the 90 percent confidence level. The level of alarm standing alone must meet a Pd of .90 at the 90 percent confidence level for the applicable intrusion scenarios at that location.

8.5.6. Priority C Resources. For priority C resources use a systems approach to provide intrusion detection for restricted areas. The goal is to put in place IDS which present significant deterrence to the unskilled intruder and enhances the benefit gained form other elements of the security system such as security patrol activity and security support force awareness. Do not request a deviation for absence of the capability if the programming process is ongoing.

NOTE: MAJCOMs will determine Pd rates for priority C resources and reflect these in applicable system security product descriptions (SSPDs).

8.5.7. Relocatable Sensors. Ideally, the AF uses sensors that can be relocated in place of fixed or permanent-fixed sensors wherever practical. These sensors must meet the IDS requirements in this chapter.

8.5.8. Invalid Alarm Rates (IARs) for IDS Associated with Priority A, B, and C Resources. As a rule, IARs should not exceed two every 24-hours, per sensor sector or zone. Invalid Alarm Rates (IARs) for IDS Associated with Priority A, B, and C Resources. As a rule, IARs should not exceed two every 24-hours, per sensor sector or zone. **EXCEPTION**: IDS configured as individual resource sensors must not exceed three IARs per 24 hours, per resource.

8.6. General Alarm Annunciation and Display Requirements for IDS Supporting Restricted Areas That Contain Nuclear Weapons. These applications require:

8.6.1. A Primary Annunciator. The primary annunciator incorporates command, control, and display components. It displays alarms generated by structure and exterior sensors; responds to operator input; allows operators to interact with AECS; activates response devices; and supports other electronic security components as required.

8.6.1.1. A primary annunciator can operate on a laptop computer, a desktop computer, a computerized workstation, and/or specific BISS alarm annunciation equipment.

8.6.2. Remote Annunciator. The remote or secondary annunciator operates through the central processing unit (CPU) serving the primary annunciator. The remote mirrors the primary annunciator's functions by displaying alarm indicators, facilities, AECS status system status, map displays and other information that shows on the primary display.

8.6.2.1. The remote annunciator must also display the status of the primary alarm operator and provide the remote system operator with the capability to take operational control of a sensored area from the primary, either by operator command or automatically upon failure of the primary annunciator.
8.6.2.2. If the primary annunciator malfunctions, security forces must be deployed to perform immediate visual assessment (IVA).
8.6.2.3. The AF accepts the potential risk associated with CPU failure in systems with a single CPU.

8.7. Specific Alarm Annunciation and Display Requirements for IDS Supporting Restricted Areas that Contain Nuclear Resources. IDS for a given area normally annunciates and displays at a single location within the restricted area (MSCF, ECF, or site security control center [SSCC]) with remote annunciation and displays at CSC or the LED. The primary annunicator must display a complete system status of all sensors, sensor sectors, or sensor zones. It must display, audibly and visually in alpha-numeric fashion, access, secure and alarms states and the changes from one state to another.
8.7.1. Map Displays. These indicators must be displayed as text and as a point on a geographic map depicting the IDS layout in relation to the restricted area configuration. Geographic map displays must indicate roads, the area perimeter, and structures in the area. (**EXCEPTIONS:**WS3.) Hand-held annunciators (HHAs) don't require area display maps.
8.7.2. Data-Link Supervision. These audio and visual indicators show hardwire or non-wire-line data-link supervision status, including warning of detected radio channel jamming.
8.7.3. Self Tests. The primary annunciator must initiate self tests of individual sensors that support such a test.
8.7.4. IDS Control at Non-US NATO Sites. See AFI 31-101, Volume 2, paragraph 4.
8.7.5. Alternate Power. IDS components requiring a primary power source such as commercial power, must also have an alternate power source using standby generators and batteries. Batteries must maintain satisfactory operation of sensors and annunciation equipment for a minimum of four hours. Switch over to alternate power sources must ensure uninterrupted operation. The alarm panel must display the switch-over as exactly that, and must not register it as a multiple intrusion alarm.
8.7.5.1. All IDS must transmit "low-battery" messages for all essential data transmission subsystem components and sensors before their functions degrade. Low-battery messages must show on the primary, remote, hand held annunciator (HHA)s, and hand held monitors (HHMs).
8.7.6. Communications Equipment Integration Capabilities. Control and display subsystems of the primary annunciator must accommodate all on-site communications media.
8.7.7. Human Factors. IDS annunciators must have display and system control functions designed to permit the operator to change alarm status, acknowledge and reset alarms, and conduct self-tests of the circuit continuity with the maximum level of efficiency. Security supervisors for areas supporting nuclear weapons will rotate the MSCFO at least every 4 hours and conduct random unannounced checks of operator
assessment by causing actual sensor alarms. Commander and managers should consider this for non-nuclear areas as well.
8.7.8. Alarm Event Priority. Computer based IDS annunciators display alarms, in order of priority. The priority of alarms is:
8.7.8.1. Individual resource or structure intrusion alarms.
8.7.8.2. Individual resource or structure tamper alarms.
8.7.8.3. Boundary intrusion alarms.
8.7.8.4. Boundary tamper alarms.
8.7.8.5. AECS alarms.
8.7.8.6. Duress alarms.
8.7.8.7. Other alarms on a first-in, first-out basis.
8.7.9. Probability of Correct Annunciation (PCA). Primary, remote and HHAs must all work with 100 percent accuracy.

8.8. Alarm Annunciation and Display Requirements for IDS Supporting Nonnuclear Priority Resources. IDS supporting restricted areas that contain nonnuclear priority resources must include a primary annunciator with the same features prescribed for those supporting restricted areas containing nuclear resources in paragraphs 8.7.1 through 8.7.9. **EXCEPTION:** The AF doesn't require a remote annunciator for nonnuclear priority resources unless it's specified in the security standard. If a remote annunciator is required, it must meet the requirements identified in Paragraph 8.7.

8.9. Hand-Held Annunciator (HHA). These portable sensor alarm data transceivers provide the same basic functions as primary or remote annunciators. Use them primarily with sensors that personnel can relocate to support deployed priority resources. You may use HHAs to support resources at bare-base or deployed locations. When used as primary annunciator, HHAs must:
8.9.1. Provide the capabilities identified in Paragraph 8.6.1.
8.9.2. Operate for a minimum of 12 hours on a single charge.
8.9.3. Operate from a vehicle 12- or 24-volt charging system, if necessary.

8.9.4. Not interfere with other base communication systems.

8.10. Hand-Held Monitors (HHM). Mobile patrols or fixed security posts use these portable alarm data receivers to enhance alarm response capabilities. HHMs don't perform the functions of primary, remote, or HHAs.

8.11. Assessment Requirements. Security forces perform assessments to determine the cause of an alarm and initiate the appropriate response.

8.11.1. Immediate Visual Assessment (IVA). All permanent restricted areas containing priority A or B resources must employ an IDS concept of operations that provides for IVA of exterior alarms either by the IDS operator using remote imagery equipment or security forces posted in the restricted area. When the IDS operator can't determine the cause of an alarm by IVA or by posted sentries, security forces must respond immediately.

8.11.2. Priority C Requirements. Security forces must provide response and alarm assessment within five minutes in areas containing priority C resources.

8.12. Transmission Line Security for Nuclear Resources. Secure alarm data transmission equipment against tampering by using data transmission line supervision features encryption, and security force surveillance within the restricted area. To secure the data transmission equipment, personnel:

8.12.1. Controlling Data Transmission. Control data transmission media with equipment such as hardwired or optical fiber data transmission links (land lines) or radio waves, both omni-directional (broadcast) and directional (microwave and light wave). If you use radio, make sure that you don't lose IDS alarms because of radio frequency interference.

8.12.2. Supervising Data Transmission. Supervise data transmissions by protecting and controlling data transmission media according to its sensitivity. Data transmission must be supervised using:

8.12.2.1. Class I supervision. Use DES or an algorithm based on cipher feedback or the cipher block chaining mode of encryption. Obtain required certification from the National Institute of Standards and Testing or another testing laboratory. MAJCOMs keep the certification for the life cycle of the system.

8.12.2.2. Class II supervision. Systems using this type of supervision include those which base transmissions on pseudorandom generated tones or digital encoding using an interrogation and response scheme throughout the entire communication, or those using UL class AA line supervision. The algorithm must not repeat itself within a minimum 6-month period. Class II security must protect a system with resistance, voltage, current, or signal substitution techniques.

8.12.2.3. When the transmission line leaves the restricted area and traverses an uncontrolled area, protect it with class I line supervision. When the transmission line remains within the restricted area, use class II line supervision.

8.12.3. Physical Protection of Internal Cabling. Installations must dedicate the cabling between the sensors and the control unit, called the detection loop, to the IDS. IDS cabling may be routed in rigid pipe (polyvinyl chloride) or equivalent raceways. These materials must comply with national electric code standards.

8.13. Physical Protection of Permanent Cabling. Physically protect permanently installed exterior communications cable data links and circuits using conduit, direct burial, or above-ground installation methods. Route exterior IDS cables that aren't directly protected by sensors through metal conduit either buried to the normal depth of the cables as stated in the siting criteria or suspended at least 10 feet (3 meters) above the surface.

8.14. Terminal and Junction Boxes. Install locks and tamper switches that provide a tamper indication to the annunciator(s) on equipment that terminates, splices, and groups interior or exterior IDS input or that could allow spoofing, bypassing, or other system sabotage. Such equipment includes permanent junction boxes, field distribution boxes, cable terminal boxes, and cabinets.

8.14.1. Securing Equipment. Seal or lock this equipment if it is located within the protection zone of the sensors. Tamper switches are not required if the equipment can be protected by sensors. Secure junction boxes located inside restricted areas but outside of structures or shelters equipped with sensors. Use recessed socket wrench bolts, screws, locks, or other hardware. he agency responsible for sensor system maintenance secures, controls, and accounts for keys to all the locks in use.

8.15. Security for Temporary or Relocatable Radio Communication Data Links. Radio communication data links used to transmit alarm system data must not transmit continuously. These systems must transmit a coded message to report an alarm, respond to a self-test command, send status messages, and relay control signals.

8.15.1. Polling Systems. Data transmission links must use a half duplex supervised polling system specifically designed for alarm data transmission. They must display the result of polling queries only when a failure occurs. Polling response time and transmission data rate, data error rate, and equipment reliability must not degrade overall IDS alarm annunciation time and PCA.

8.15.2. Protecting Radio Frequency Data Transmission Equipment. Protect radio frequency alarm data transmission equipment, including repeaters, at the same level of security as you give to the remaining alarm data communications network. Protect them with a local sensor detection zone or other physical security techniques and tamper protection. Security systems must detect, transmit, and indicate tamper alarms for all components and sensors.

8.16. Environmental Requirements. Use rugged and corrosion-resistant IDS components. Exterior components must operate satisfactorily in a maximum rainfall of 2 inches per hour. Portable components must be quickly configured without sophisticated tools or support equipment.

8.17. System Sharing. When an installation uses different types of data transmission links, they must interface with each other.

8.18. Radio Frequencies. For radio frequency data transmission links, the security system must operate in all worldwide frequency bands designated in the International Telecommunications Union and National Telecommunications and Information Administration, Table of Allocations. The security system must use dedicated frequencies to transmit IDS alarm data. It muss detect and report intentional and unintentional jamming attempts. It must transmit IDS alarms sent by non-hardwire links even when they occur during "off-air" periods caused by maintenance or failure.
8.18.1. Routing Data Transmissions. Require primary and alternate routes for data transmission and system control. If you use radio for both methods of data transmission, use different frequencies.

8.19. Radio Frequency Link Compatibility. Data transmission subsystems using radio frequency methods must transmit on one or more of the frequencies within the specified band. These transmissions must not interfere with other IDS components or any electronic components within the area. Examples of these are, but are not limited to electric circuits; motors; transformers; ignition systems; heating sources; static, weather, and other radio frequency signals.
8.19.1. Configuring Radio Frequency Transmitters. Configure radio frequency transmitters according to the requirements in Federal Communications Commission Rules and Regulations, Title 47, Part 90, *Private Land Mobile Radio Services*, Oct 93.

8.20. Radio Frequency Transmission of IDS Signals for Nonnuclear Priority Resources. Transmit radio frequency data of IDS alarms for nonnuclear priority resources using:
8.20.1. Automated Communication Link Supervision. IDS alarm data transmission equipment must automatically (through "polling" or "one-way state of health tracking") track the condition of the communication link. It must annunciate separate, distinct alarms for; communication link malfunctions; jamming or interference; and intrusions.
8.20.2. Frequency Management. Use alarm data transmission equipment that you can tune to multiple frequencies. This feature mitigates frequency management problems. The radio frequency communication link must not interfere with; other IDS components; aircraft; vehicles; communications; other equipment used for military operations.

8.21. Test and Exercise Requirements. Test and certify newly installed IDS before operating them as a line or level of detection. MAJCOMs ensure:
8.21.1. The installing agency works with the operating agency to perform an initial 72-hour checkout of the system before turning it over to the user.
8.21.2. After the 72-hour test, the user performs a 30-day operational test based on the acceptance test plan. Obtain this plan from the Electronic Sensor Equipment Program Office, ESC/AVJB, 20 Schilling Circle, Hanscom AFB MA, 01731-2816 through the MAJCOM/SP.
8.21.3. During the 72-hour test, SP must thoroughly investigate the capabilities and limitations of the system to establish a baseline of expectations in regard to invalid alarms.
8.21.4. When the sensor system supports nuclear resources, after the 30-day test the system must undergo an Initial Nuclear Surety Inspection (INSI) required by AFI 90-201, *Inspector General Activities*, prior to operational use. The MAJCOM inspector general, or when delegated, the MAJCOM SP staff, tests and certifies the system in writing.
8.21.5. When the sensor system supports nonnuclear resources, the MAJCOM SP staff:
8.21.5.1. Conducts a certification test for priority A resources.
8.21.5.2. Certifies the system for operational use, in writing.
8.21.5.3. Delegate certification testing for priority B and C resources, if necessary, to the NAF staff or the ISC and provide the testing criteria.

8.22. Operational Test and Evaluation (OT&E). The AF/SP determines the level of testing required to approve new or modified IDS. Normally, OT&E is required for major system components. Once an IDS component is approved for follow-on

deployment. However, users must conduct a functional and operational test of the system to ensure it meets acceptance standard.

8.23. Sensor Performance Test Requirements..

8.23.1. Quarterly Testing. At least once each quarter security, police supported by sensor maintenance personnel, conduct a walk-through test of each storage structure or aircraft shelter IDS and each individual resource IDS. This test will ensure compliance with system technical order specifications, that the sensors react to basic intrusions, and to determine whether environmental changes or resource reallocations have affected sensors.

8.23.2. Nonnuclear Testing. Check structures or shelters that routinely contain nonnuclear priority resources quarterly. Test randomly until you check all structures or shelters. If you must store nuclear resources in these structures or shelters, conduct a walk-through test before relying on the sensor system.

8.24. Periodic Test Requirements.

8.24.1. Exterior IDS. Test randomly selected sectors of the exterior IDS daily by causing an actual alarm. When conducting the test, use the procedures in the applicable T.O. Select the sensor sectors and zones so that you test the entire exterior IDS at least monthly.

8.24.2. Operational. When again using sensors that have been deactivated, conduct complete operational testing as required in paras 8.23 and 8.24 of this instruction.

8.24.3. Two-person BISS maintenance concept for IDS supporting nuclear resources. A two-person maintenance team integrity concept for selected BISS security subsystems (access to the coder multiplexer sensor data (CMSD), field distribution boxes (FDB), and terminal boards/boxes where sensor cable pairs are routed, and computer based annunciator systems) is required. This applies to both normal duty hours and “on-call” BISS maintenance. Do not confuse this requirement with the nuclear surety standards for nuclear weapons outlined in the AFI 91-series. Although every effort will be made to preclude BISS maintainers from separating from one another during these tasks, they may separate without violation of the nuclear surety two-person rule.

8.24.4. Because the CMSD, FDBs, terminal boards, and computer based annunciators are critical nodes, if maintainers become separated, all work performed on these systems will be reviewed by the second team member before the job is completed. (Designed to prevent an obvious manipulation of the system that can be recognized by a simple review)

8.24.5. Maintenance and security personnel must conduct an operational walk test of each line fault or sensor alarm message (SAM) received as a result of maintenance activity. All alarms, even those received from outside the serviced zones, accidentally caused by maintenance, will be walk tested by security forces when servicing is completed. This requires alarm operator familiarity with the nature of maintenance being performed and potential for exploitation at each critical maintenance node. Locally devised quick reference aids, showing sensor line routing through critical maintenance nodes are recommended. Classify these aids appropriately.

8.24.6. When servicing key nodes as described, security forces will assist BISS maintenance personnel to the fullest extent possible.

8.25. Tamper Switch Test Requirements.

8.25.1. Tamper Tests for Sensors Supporting Nuclear Resources.

8.25.1.1. Test tamper switches located within an IDS zone of coverage, i.e., a person cannot gain access to the equipment without being detected by the exterior or structure IDS (including WS3 systems and individual sensor heads), at least annually.

8.25.1.2. Test all other tamper switches at least quarterly.

8.25.2. Tamper Tests for Sensors Supporting Nonnuclear Resources. Test tamper switches at least quarterly.

8.26. Vulnerability (Adversarial) Testing. IDS testing identifies and mitigates any system vulnerabilities to ensure that the system continues to detect and assess intrusions effectively. In addition to tech order testing, subject IDS to various adversarial or feasible “real-world” intrusion scenarios to determine overall system performance, reliability, working status, and availability. The results of these tests give the user a complete assessment of the IDS. Conduct tests during all phases of a system’s life cycle.

8.26.1. Test Measurement. Test IDS components to ensure that security forces can assess and respond in a timely manner. Specific measures of IDS effectiveness and evaluation criteria include:

8.26.1.1. Pd and confidence levels. (Applies to new or significantly modified alarm systems)

8.26.1.2. Correct annunciation.

8.26.1.3. Correct assessment.

8.26.1.4. Vulnerability of IDS to surreptitious intrusions.

8.26.1.5. Reviews of the IAR.

8.26.1.6. Availability and reliability of alternate power support.

8.26.1.7. Access delay and denial.

8.26.2. Constructing Scenarios. Base scenarios on the DoD postulated threat and other identified threats. Conduct scenarios, consisting of single and multiple intruders, on primary and alternate power systems, during all types of weather, during daylight and at night. Use system limitation data identified in para 8.2.2. above to design adversarial testing scenarios. Results of the tests are not less than DoD unclassified controlled nuclear information (UCNI) when conducted in restricted areas containing nuclear weapons.

8.26.3. Test Requirements. Units must conduct quarterly vulnerability tests to validate the IDS capabilities and limitations. The results of vulnerability tests form the basis for reporting security deficiencies to HQ USAF/SP, according to Paragraph 1.26, and DoD 5210.41-M requirements.

8.27. Criteria for Evaluating Sensor Equipment. Vary the size and weight of the individual conducting the tests. At a minimum, test system vulnerability for boundary sensors using:

8.27.1. Balanced Magnetic Switch (BMS) Exception. BMSs located on storage structure doors that you must jack up to open need not meet the exact tolerance of 1-1/4 inches as long as the BMS indicates an intrusion before an intruder could open the doors enough to tamper with the alarms or gain access to the structure.

8.27.2. Long Ported Coaxial Sensor Cable and Short Ported Coaxial Cable. These cables detect intrusions from running, walking, crawling, and jumping. Test the system using normal movements from very slow to fast. To test whether the system covers the designated area, attempt to walk around or zigzag through cable connections and areas where cables and other sensors overlap (that is, where RACON coverage for gates begins). Attempt to jump across the sensor field.

8.27.3. Bird Eye and RACON. These detect intrusions from running, walking, crawling, and jumping. Test using all intrusion methods. Attempt to walk through, between, and around the beams. Pay particular attention to areas around sensor junctions to ensure that there is no gap in coverage. Attempt to jump and crawl around the sensor field.

8.27.4. MAID/MILES. These detect intrusions from running, walking, crawling, and jumping and also detect ferrous metals. Test according to paragraph 8.27.2 but add ferrous metal testing. For example, cross the sensor field with metal plated boots, and without metal plated boots while carrying metal tools or weapons at, below, and above the waist level. Also use plastic or nonmetallic tools to discriminate between seismic or metal sensor activation. Attempt to jump across the sensor field.

8.27.5. Inertia Guard. Since this sensor detects cutting and climbing, conduct scenarios to simulate cutting and aided and unaided climbing. One example to test cutting detection includes weaving 9-gauge wire through fence fabric then cutting the woven wire. Do all tests in a non-destructive manner. Attempt to climb the fence using aided and unaided scenarios. Check all areas (high and low) of fence, including corner braces, posts, and supports. Pay particular attention to areas below anti-ram cables, if installed. Test fabric by having an individual lean against the fence and push it taut while a second person attempts to cut it.

8.27.6. FPS II and E-FLEX. Test as for inertia guards, Paragraph 8.27.4. Attempt to remove the sensor from the fence fabric by cutting the wire ties that attach the sensor.

8.27.7. Fence Disturbance Sensor. This detects climbing. Climb the fence at various locations, including at the center and at the posts. Climb corner posts and jump off. Vary rates of climbing speed, weight, and size of individuals conducting the tests.

8.27.8. DTR-90. This detects climbing. Attempt to climb over a fence by straddling the DTR-90 without setting it off. Climb on fence posts and corner braces. Pay particular attention to corners and angles of less than 90 degrees. Attempt to separate wire strands far enough apart and climb between them without activating the alarm. These procedures also apply to the "Y" and vertical DTR-90 configurations.

8.28. Annunciation and Display Equipment Tests. Alarm system operators check the annunciation and display equipment at each shift change to determine the status of the system. Operators conduct a test of the remote circuit continuity at each shift change, if the annunciator can do so.

8.28.1. Proficiency. Supervisors must conduct proficiency exercises at the remote display location to give the operator an opportunity to maintain proficiency and to simulate conditions under which the remote location would assume the duties of the primary annunciation and display location.

8.29. Operations and Maintenance. Security supervisors must make sure that personnel report system malfunctions promptly.

NOTE: Treat instructions in Paragraphs 8.21 through 8.35 as UCNI when associated with specific restricted areas containing nuclear weapons. Document maintenance on:

8.29.1. Air Force Technical Order (AFT) Form 781A, *Maintenance Discrepancy and Work Document.*

8.29.1.1. Security police record maintenance discrepancies, such as system tests and false or nuisance alarm data, separately from day-to-day activities. Use AFTO Form 781A or equivalent contractor form, if applicable. Maintain AFTO Form 781A to record an open (uncorrected) discrepancy at the MSCF. Notify the unit sensor NCO of all discrepancies by the following duty day. When you complete the form and clear the system of open discrepancies, send all copies of AFTO Form 781A to the unit sensor NCO.
8.29.1.2. The unit sensor NCO keeps, controls, and disposes of the form according to Air Force Regulation (AFR) 12-50, Vol 1, *Disposition of Air Force Documentation-Policies, Procedures, and Responsibilities* (AFI 37-133V1).
8.29.2. Air Force Form 340, *Sensor Alarm Data.*
8.29.2.1. After initially installing a system, record all alarm data on AF Form 340 or keep an annunciator printout, if available.
8.29.2.2. Installation SP, communications, and civil engineering personnel must analyze IARs that exceed the established average rate for the subsystem. Send this analysis and recommendations to the MAJCOM/SP.
8.29.2.3. MAJCOM/SP decides whether to repair or accept the high IAR and reports accepted problems to HQ USAF/SPX.
8.29.2.4. Units continue to monitor, record, and carefully track problem sensors until they bring IARs to within the average rate or until the MAJCOM/SP/SC, working with HQ USAF/SPX, accepts the high IAR for the system's life cycle.
8.29.2.5. The remote display operator must keep track of all alarms and actions occurring at the MSCF. This ensure no loss of capabilities should the primary annunciator lose detection capability.
8.29.2.6. Keep IDS data for 1 year in order to seasonally average the alarm rate.

8.30. Performance Reporting. Units using sensor systems must give MAJCOMs periodic performance reports. These include follow-on reports on IDS performance after installation. Units must also provide spot reports when failures or malfunctions occur or when local personnel can't determine or correct the cause of a failure.
8.30.1. Reporting Requirements. Submit reports on IDS installation and failure outlined in 8.27 and this paragraph via RCS report (RCS: HAF-SPO [(AR) 9346]), *Intrusion Detection Equipment Performance Report*. Report sensor vulnerabilities outlined in Paragraph 8.26.3 via RCS report (HAF-SPO (AR) 9347), *Sensor Vulnerability Report.*
8.30.1.1. Continue reporting during emergency conditions using emergency status code C-1, Priority.
8.30.1.2. Continue reporting during MINIMIZE.
8.30.13. After installing IDS, send an initial performance report to the MAJCOM/SP. This report establishes baselines for performance and IAR.
8.30.1.4. MAJCOMs determine the need for any further reporting requirements for performance analysis.
8.30.1.5. If a catastrophic failure or major malfunction condition exists for 72 hours or more, send a coordinated SP and information systems message report to the MAJCOM/SP outlining:
8.30.1.5.1. The nature of the problem.
8.30.1.5.2. Corrective actions underway.
8.30.1.5.3. Estimated time of correction
8.30.1.6. Forward sensor tests that identify potential vulnerabilities to HQ USAF/SP through the appropriate MAJCOM by message as soon as personnel discover the vulnerability. Clearly state the type of test performed and the vulnerability discovered. Identify any solutions that you've used to eliminate the vulnerability. As appropriate, classify the problem according to the BISS Classification Guide.

8.31. Technical Orders.
8.31.1. Maintaining T.O.s. The sensor NCO must maintain T.O.s and commercial manuals that describe equipment components and operating procedures for IDS in use. Sensor NCOs must have on hand:
8.31.1.1. The T.O.s that make up the Numerical Index Reference Table.
8.31.1.2. T.O. 00-35D-54, *USAF Materiel Deficiency Reporting and Investigating System*
EXCEPTION: Security police units need not maintain the T.O.s and commercial manuals if they have 24-hour access to them at another agency, such as the communications squadron.

8.32. Standardization and Training. The sensor NCO helps the standardization and evaluation section to develop certification standards for system operators.

NOTE: Only personnel possessing special experience identifier (SEI) 323 will be certified to perform MSCFO duties.
8.32.1. Security forces use these standards to evaluate unit proficiency and to identify areas needing more training or emphasis.
8.32.2. MSCFOs must take a quarterly no-notice test that evaluates their actions when confronted with a sensor activation message caused by an attempted intrusion. Test failure results in immediate decertification.
8.32.3. Standardization and evaluation personnel conduct these tests and coordinate them with element supervisors.

8.33. IDS Management. A full-time SP sensor NCO must work at installations employing sensor systems that support priority resources.
8.33.1. Security supervisors must review the operational status of their sensor subsystems.
8.33.2. The weapons system security superintendent must conduct joint quarterly walk-through inspections with BISS maintenance personnel and the sensor NCO, to check IDS:
8.33.2.1. Structure.
8.33.2.2. Shelter.
8.33.2.3. Individual resources.
8.33.2.4. Exterior sensor systems.

8.34. IDS Failure. Assess the severity of IDS failure against IDS failure categories listed in Paragraphs 8.34.1 through 8.34.4. (See Paragraph 8.30 for reporting requirements.)
8.34.1. Catastrophic Failure. Catastrophic failure occurs when the entire system or a major portion of it is inoperative. For example, a complete failure of the annunciator or display.
8.34.2. Major Malfunction. Major malfunctions occur when:
8.34.2.1. A failure could allow an intruder to penetrate a restricted area boundary without crossing at least one line of detection.
8.34.2.2. The structure and shelter or individual resources IDS components fail.
8.34.2.3. Either the primary or alternate annunciator and display equipment is inoperative.
8.34.2.4. The remote location can't monitor the primary location.
8.34.3. Partial Failure. Partial failure occurs when:
8.34.3.1. A failure could allow an intruder to cross only one line of detection at areas with two lines of detection at the boundary.
8.34.3.2. A portion of the line of detection fails at the IDS entrance or the interior.
8.34.4. Annunciator Failure. Annunciator failures occur any time the primary or remote annunciator supporting a restricted area containing nuclear weapons isn't operational. When an annunciator fails, post a second individual qualified to operate the sensor system at the operational location to protect against unauthorized IDS deactivations. Continue to use the MSCF if it helps make individual visual assessments (IVA) of exterior components.

8.35. Sensor System Compensatory Measures. When any portion of the IDS fails or has been accessed, compensate for the lost portion. Compensatory measures depend on the severity of the failure. Tailor them to make up for the lost capability. At a minimum, take the compensatory measures in Figure 8.1 when parts of the exterior sensor system in areas containing nuclear weapons break down. MAJCOMs must determine the minimum compensatory measures for systems supporting nonnuclear resources.

Figure 8.1. Compensatory Measures for Systems.

System Components	Status?	Alarm System Compensatory Measures Implemented
Fence alarm functional	Yes	1. Provide constant surveillance for the affected area.
Clear Zone alarm functional	No	2. Check adjoining sectors to ensure that they function properly.
Clear Zone alarm functional	Yes	1. Send ART to each alarm to confirm MSCFO assessment.
Fence alarm functional	No	2. Check adjoining sectors to ensure that they function properly.
Fence alarm functional	No	1. Post CBSs.
Clear Zone alarm functional	No	2. Check adjoining sectors to ensure that they function properly.

PART 3
AIR FORCE PRIORITY RESOURCES AND STANDARDS

Chapter 9

STANDARD FOR COMMAND, CONTROL, COMMUNICATIONS, AND COMPUTER (C4) SYSTEMS

9.1. Physical Security Requirements. Determine physical security requirements for communications assets by reviewing their total contribution to the Air Force's warfighting capabilities. Alternate routes in the network can minimize the need for stringent security applications. Possessing MAJCOMs:

9.1.1. Identify and maintain a list of each C4 asset currently assigned a security priority based on previous directives and regulations.

9.1.2. Implement security measures to ensure that personnel safeguard vital C4 assets at a level commensurate with their relative importance to the mission.

9.1.3. Propose the priority changes and designations for communications systems based on the relationship between the C4 asset and the resource it supports. Also consider the degree of redundancy or alternate routing characteristics.

9.1.4. Need not request AF/SP approval of C4 priority revisions needed as a result of approved security priority changes to the resources they directly support.

9.2 Security Forces. MAJCOM/SP works with MAJCOM/SC/DO to plan and implement security posts and patrol coverage for on- and off-base facilities containing C4 systems. (See Chapter 1 for guidelines.)

9.2.1. Armed C4 system owners and users require training in armed defense methods.

9.2.2. Designate the security control function to a continually manned position, such as CSC or LED.

9.2.3. Support off-base sites with an armed response capability, such as:

9.2.3.1. USAF SP.

9.2.3.2. Contract guard (where current law "grandfathers" contract services).

9.2.3.3. DoD Guard.

9.2.3.4. Local or host-nation police or military.

9.2.4. When you assign contractor employees security tasks, you must include appropriate tasking and outline training requirements in the contract. If you draw up a classified contract, comply with the investigative and security clearance requirements of DoD 5220.22-R, *Industrial Security Regulation,*and AFI 31-601, *Industrial Security Program Management.* Otherwise, apply personnel security directives.

9.3. Security Facilities. In addition to the requirements in this instruction, apply additional security requirements, including:

9.3.1. Boundary Barriers. Off-base restricted areas for priority C facilities need a substantial boundary barrier. The AF recommends type A fencing.

9.3.1.1. Secure Entrances into Facilities. Externally reinforce wooden doors with US 16-gauge sheet cover, installed to prevent easy removal. Peen and weld hinge pins. Construct windows and vents to prevent forced entry. Bar and secure them with chain-link or expanded 9-gauge or higher gauge metal securely fastened to the window casing or wall to prevent its removal. Build walls of substantial material.

9.3.1.2. MAJCOMs:

9.3.1.2.1. Determine when fence installation is impractical due to terrain, climate, socio-political sensitivities, or other factors.

9.3.1.2.2. Specify restricted area sign placement.

9.3.2. Vegetation Control. For priority C off-base C4 facilities, MAJCOMs determine vegetation requirements. (See Paragraph 7.6.2.)

9.3.3. Lighting and Lock Requirements.

9.3.3.1. Provide entry point lighting for all C4 priority resource facilities according to Chapter 7. Lock or alarm:

9.3.3.1.1. Manhole covers.

9.3.3.1.2. Cable vaults.

9.3.3.1.3. Junction boxes.

9.3.3.1.4. Water and fuel filler pipes that provide entry to utilities and cable routes serving facilities secured under this instruction.

9.3.3.1.5. Facilities housing alternate power sources.

9.3.3.2. MAJCOMs must specify the type of lock.

9.3.3.3. When possible, put utilities underground or encase them in hardened conduit. Bury or rivet fuel and water tanks and lines and lock fuel and water filler caps.

9.4. Survivability Measures. Establish these measures according to owner MAJCOM requirements and DoD 5200.8-R.

9.5. Security Procedures and Plans. Incorporate security plans for C4 facilities and sites in the ISP. When a non-USAF host agency supports a site or facility, incorporate security plans in appropriate agreements with host-nation civil or military agency.

Chapter 10

STANDARD FOR DOD SPACE LIFT SATELLITE CONTROL, DETECTION

10.1. Overview. This chapter outlines security priorities and guidelines for space system assets located on AF installations or in the control of AF personnel.

10.2. Security Force Requirements. The number of security forces assigned to secure space assets depends on the:
10.2.1. Threat to the mission.
10.2.2. Mission priority.
10.2.3. Mission location.
10.2.4. Physical security facilities and equipment available.

10.3. DoD Spacelift and Space Launch Systems (SLS) Security Priorities. Security Priorities are assigned as indicated in figure 10.1.

Figure 10.1. Security Priorities for DoD Spacelift and Space Launch Systems.

Restricted Areas Containing These Types of Facilities and Equipment:	Security Priority
Operational USAF Space Launch Complex (SLC) when both the space launch vehicle and payload are on site.	A
Essential command and control, communications, or computer facilities (for which no backup exists) engaged in direct support of critical space launch operations.	A
Operational USAF Space Launch Complex (SLC) when either the launch vehicle or payload are on site without meeting the priority A criteria of simultaneous presence.	B
Essential launch and payload processing facilities or equipment for which no backup capability exists.	B
Essential launch and payload processing facilities or equipment with backup capability.	C
Booster and flight hardware storage areas when hardware is present.	C
Hypergolic fuel storage and processing areas.	C
NOTE: Flight hardware is defined as mission equipment used in support of the launch vehicle, payload, upper stages, spacecraft, carrier, and other equipment required to perform the mission.	

NOTE: Refer to paragraphs 1.3.2., 1.4.2., and 1.5.2. for general entry control, boundary detection and surveillance, and RF security requirements. Chapters 7 and 8 provide general physical security and IDS requirements. Refer to paragraph 10.10. for specific requirements.

10.4. Space Systems Responsibilities. The Director, Office of the Secretary of the Air Force, Office of Special Projects (SAFSP) serves as the Executive Agent of the Secretary of the AF for designated space launches and command and control systems. Further, this position oversees security policies, requirements, and standards for SAFSP resources.

10.4.1. Office of Primary Responsibility (OPR). SAFSP serves as the OPR for SLSs and command and control resources owned exclusively by OSAFSP , including:

10.4.1.1. Flight hardware.

10.4.1.2. Ground support equipment.

10.4.1.3. Facilities.

10.4.1.4. Software.

10.4.2. The Director, SAF/SP:

10.4.2.1. Identifies and oversees all matters relating to SAF/SP resources at Vandenberg (AFB), CA, Cape Canaveral Air Force Station (AS), FL and other classified locations.

10.4.2.2. Coordinates the level of security with HQ AFSPC/SP and HQ USAF/SP.

10.4.3. Installations provide:

10.4.3.1. Entry control, boundary surveillance, and at least one ART for restricted areas containing priority A resources.

10.4.3.2. Entry control and at least one ART for restricted areas containing priority B resources.

10.4.3.3. An ART for restricted areas containing priority C resources.

10.4.3.4. Entry control, boundary assessment, and armed response for marshaling areas containing priority resources.

10.4.3.5. An SRT to accompany the tow vehicle during convoys.

10.4.4. Owning and using installations:

10.4.4.1. Maintain and monitor installed IDS that secure internal SAFSP areas.

10.4.4.2. Request armed security forces to investigate all boundary alarms.

10.4.4.3. Work with the host SP to monitor exterior IDS.

10.4.5. The SAFSP program security office (PSO):

10.4.5.1. Represents SAFSP.

10.4.5.2. Specifies security requirements for SAFSP payloads stored in restricted and unrestricted areas and provides an EAL to personnel controlling entry.

10.4.5.3. Establishes and administers procedures for SAFSP personnel and aerospace payload support contractors entering and enrolling in SAFSP areas.

10.4.6. The SAFSP Operating Location (OL/A) Commander represents SAFSP and:

10.4.6.1. Approves any request to photograph, videotape, or reproduce images in any media of SAFSP resources.

10.4.6.2. Works with the PSO to approve any release of the data.

10.4.6.3. Modifies flying directives and procedures to announce prohibitions against reproducing images.

10.4.6.4. Controls mapping, charting, and geodesy activities and procedures to ensure that personnel coordinate their work in advance.

10.4.6.5. Coordinates work on audiovisual systems publications dealing with:

10.4.6.5.1. Official and unofficial photography;

10.4.6.5.2. Local LE and security directives or procedures designed to guard against photography;

10.4.6.5.3. Local public affairs activities, directives, and procedures.

10.4.6.6. Coordinates work with other Federal, state, and local agencies to place appropriate warning signs at strategic locations, enforce a closed-base policy, and take similar enforcement measures.

10.4.6.7. May authorize a temporary deviation for up to 90 days consistent with paragraph 4.6.1 of this instruction.

10.5. Other Space and SLSs. All military and commercial spacelift operations using AF facilities, property, and equipment must comply with the standards in Paragraphs 10.5.1 and 10.5.2.

10.5.1. Payload Security. Responsible payload personnel:

10.5.1.1. Work with HQ AFSPC and all affected organizations to develop payload security standards with security priority and payload-unique requirements.

10.5.1.2. Coordinate changes to the standards with HQ AFSPC and affected organizations.

10.5.2. Security Requirements and Procedures. HQ AFSPC develops and distributes specific requirements and procedures for launch systems.

10.6. Space Satellite Control Systems. Space satellite control systems with unique physical features missions, threats, or site vulnerabilities, may warrant special physical security considerations. Security priorities are assigned in accordance with Figure 10.2.

Figure 10.2. Security Priority for Space Satellite Control Systems.

Restricted Areas Containing These Types of Facilities and Equipment:	Security Priority
Defense Satellite Communications System (DSCS) earth/ground terminals located OCONUS unless otherwise designated.	A
DSCS Sun East and Sun West antennas at Onizuka AFB, CA.	A
DSCS terminal at Falcon AFB, CO.	A
NOTE: DSCS earth/ground terminals located in the CONUS use the same priority as the command and control or warning systems supported.	
The 50th Space Wing's command post.	B
All data link terminals.	B
Mission communications.	B
Global positioning systems (GPS) master control stations.	B
Milstar operations centers.	B
Milstar Satellite Operations Complex.	B
Remote tracking sites (RTS) at: Vandenberg AFB, CA, New Boston AFS, NH; Thule AB, Greenland; Anderson AFB, Guam; and Kaena Point, HI.	B
Remote Tracking Sites at Seychelles, Indian Ocean; Falcon AFB, CO; Diego Garcia and Oakhanger, UK.	C
Satellite Operations Centers.	C
Resource Control Centers.	C
GPS Monitor Stations.	C
Phase 1 Backup Master Control Station.	C
Defense Meteorological Satellite Program (DMSP) locations.	C
NOTE: Assign Milstar Constellation Control Stations and terminals the same priority as the host they support.	

NOTE: Refer to paragraphs 1.3.2., 1.4.2., and 1.5.2. for general entry control, boundary detection and surveillance, and RF security requirements. Chapters 7 and 8 provide general physical security and IDS requirements. Refer to paragraph 10.10. for specific requirements.

10.7. Detection and Warning Systems. Systems with unique physical features, missions, threats, or site vulnerabilities, may warrant special security considerations. Security priorities are assigned in accordance with Figure 10.3.

Figure 10.3. Security Priority for Detection and Warning Systems.

Restricted Areas Containing These Types of Facilities and Equipment:	Security Priority
Sea Launched Ballistic Missile Detection and Warning Sites.	A
Perimeter Acquisition Radar Attack Characterization System.	A
PAVE Phased Array Warning System sites.	A
Ballistic Missile Early Warning System sites.	
North American Aerospace Defense Command Cheyenne Mountain Complex.	A
North Warning System.	B
Distant Early Warning line sites.	B

Restricted Areas Containing These Types of Facilities and Equipment:	Security Priority
North Atlantic Defense System, including the Command and Control Centers at Keflavik Naval Station, IC; Alaska ROCC, Elmendorf AFB, AK, and the South ROCC, Howard AFB, PN.	B
CONUS ROCC, Tyndall AFB, FL. Operational Tethered Aerostat Radar Systems and Sector Operational Control Centers at Griffiss AFB, NY, Tyndall AFB, FL, March AFB, CA, and McChord AFB, WA.	C C

NOTE: Refer to paragraphs 1.3.2., 1.4.2., and 1.5.2. for general entry control, boundary detection and surveillance, and RF security requirements. Chapters 7 and 8 provide general physical security and IDS requirements. Refer to paragraph 10.10. for specific requirements.

10.8. Passive Space Surveillance Systems (PASS). Figure 10.4 prescribs physical security procedures for PASS Systems. PASS comprises the Deep Space Tracking, and Low Altitude Space Surveillance (LASS) Systems. Security priorities are assigned in accordance with Figure 10.4.

Figure 10.4. Security Priority for Passive Space Surveillance Systems (PASS).

Restricted Areas Containing These Types of Facilities and Equipment:	Security Priority
PASS missions. (Some PASS systems may not be assigned a security priority.) Mechanical radar at Pirincirlik AS, TU.	A A
The PASS at Eglin AFB, FL.	C
Controlled Areas Treat ground-based Electro-Optical Deep Space Surveillance Systems as controlled areas.	

NOTE: Refer to paragraphs 1.3.2., 1.4.2., and 1.5.2. for general entry control, boundary detection and surveillance, and RF security requirements. Chapters 7 and 8 provide general physical security and IDS requirements. Refer to paragraph 10.10. for specific requirements.

10.9. Other Space Support Resources. Defense Support Program (DSP), Global Positioning Systems (GPS), and Overseas Ground Stations (OGS). Security priorities are assigned in accordance with Figure 10.5.

Figure 10.5. Security Priority for Other Space Support Resources.

Restricted Areas Containing These Types of Facilities and Equipment:	Security Priority
The European Ground Sation Overseas Ground Station. CONUS ground station and its associated space operations center, data reduction center, satellite readout station, communications center, ground communication links, maintenance room, mission essential antennae environmental control equipment, power production facilities, and water supply facilities within the restricted area. The mobile ground system main operating base.	A A A A

Restricted Areas Containing These Types of Facilities and Equipment:	Security Priority
The AN/MSQ 118 and AN/MSQ 120 trailers, when deployed. *NOTE:* Remove the security priority when you send a mobile asset for maintenance, when it is in transit to maintenance facilities, or is inoperable.	
GPS monitor stations and ground antennae.	C
Overseas Ground Station. *NOTE:* The host country provides security for OGS.	

NOTE: Refer to paragraphs 1.3.2., 1.4.2., and 1.5.2. for general entry control, boundary detection and surveillance, and RF security requirements. Chapters 7 and 8 provide general physical security and IDS requirements. Refer to paragraph 10.10. for specific requirements.

10.10. Security Force and Physical Security Requirements, and Procedures. The operating MAJCOM will:
10.10.1. Specify security posts and response force requirements, and any unique security force manning requirements. Coordinate funding for manpower authorizations with the possessing command.
10.10.2. Provide special security measures, when necessary, based on unique mission, locations, or other factors.
10.10.3. Address and coordinate with the possessing command, additional physical security facility and equipment requirements, such as:
10.10.3.1. Fencing and clear zones;
10.10.3.2. Perimeter and area lighting;
10.10.3.3. CCTV systems;
10.10.3.4. IDSs and annunciator location requirements;
10.10.3.5. Security force primary and alternate control centers;
10.10.3.6. Communications requirements;
10.10.3.7. Personnel clearances;
10.10.3.8. Duress procedures and;
10.10.3.9. Entry control procedures.
10.10.4. Specify equipment, requirements, and security procedures for convoy deployments.
10.10.5. Possessing commands and installation commanders must address unique security procedures such as badge issue, visitor control, and privately owned vehicle use, in supplements to this instruction or in site directives.

NOTE: Consult the DSP classification guide before developing local DSP security plans.

Chapter 11

STANDARD FOR NUCLEAR RESOURCES

11.1. Overview. This chapter outlines the AF implementing instructions for securing nuclear resources in transit, mated to missile systems, and in various storage areas.
11.1.1. Use DoD 5210.41-M with this instruction for all nuclear security compliance requirements. Nuclear resources are always priority A.
11.1.2. The owning MAJCOM, in coordination with the host MAJCOM, if applicable, may set up additional security requirements and procedures in supplements to this instruction.
11.1.3. Security planners apply the guidelines in AFH 31-103, *Physical Security*.

11.2. Intercontinental Ballistic Missile Systems.
11.2.1. Planning. HQ AFSPC formulates plans and procedures to safeguard strategic missile weapon systems according to DoD and AF policy.

11.2.2. Response Times. The Chief of Staff, through HQ AFSPC/CC establishes security force composition and minimum response times for missile launch facilities consistent with DoD 5210.41-M.
11.2.3. Priority A. Use priority A for launch facilities (LFs) with missile reentry systems (RS) and reentry vehicles (RVs) present, and missile alert facilities (MAFs) with manned on-alert launch control centers (LCCs).

NOTE: Don't assign a security priority to LFs with no RS or RV present and MAFs with non-alert LCCs. Control these according to appropriate weapon system safety rules. Store missile frames, if possible, in controlled areas and protect them with random patrols or more stringent coverage.
11.2.4. Security Force Requirements. See AFI 31-101, Volume 2, paragraph 5.
11.2.5. Support Facilities. In addition to the requirements outlined in DoD 5210.41-M, or as described in this chapter, support facilities require:
11.2.5.1. LFs:
11.2.5.1.1. Use low-intensity pole mounted lighting to illuminate personnel entry areas, launcher door, and nearby areas. Use sufficient illumination to quickly locate intruders.
11.2.5.1.2. Need not meet fencing requirements in Paragraph 7.4 but must provide a substantial barrier and legal boundary for the restricted area.
11.2.5.2. MAFs:
11.2.5.2.1. Provide a single gate for personnel and vehicles at the boundary fence secured by an electric lock controlled by the flight security controller (FSC).
11.2.5.2.2. Provide lighting illuminating the entry point, parking area, and approaches to the MAF support building.
11.2.5.2.3. Build fencing providing a substantial barrier and legal boundary for the restricted area.
11.2.5.2.4. Equip an MAF support building with a security control center (SCC) located above the LCC containing the elevator shaft entrance door.
11.2.5.2.5. Design SCCs to allow a single individual to efficiently control all security operations.
11.2.5.2.6. Install IDS on the elevator shaft to detect unauthorized entry. The system must include visual and audible alarm reporting in the LCC.
11.2.5.2.7. Install SCC doors that close automatically and have an electric lock the FSC controls.
11.2.5.3. Missile support installations:
11.2.5.3.1. Provide a missile security control (MSC) facility housing all equipment needed to control the security operation for the entire missile complex.
11.2.5.3.2. Set up a Keys and Codes Control Center with physical separation of the A and B side controllers. Provide A and B side controllers a system to notify WSA, CSC, or the LED of duress situations.
11.2.6. Entry Control Procedures. See AFI 31-101 Volume 2, paragraph 5, Chapter 6 of Volume 1, and DoD 5210.41-M.
11.2.7. Contractor-Controlled Facilities. Secure LFs or MAFs turned over to contractors for modification in accordance with this instruction, MAJCOM supplements, and other applicable AF directives. Industrial security instructions contain basic guidelines for determining entry and investigative requirements for contractor personnel.
11.2.8. Alarm Response Procedures. The HQ AFSPC must develop detailed alarm response procedures and include them in MAJCOM and unit supplements to this instruction.
11.2.9. LF and MAF Physical Security Checks. See AFI 31-101 Volume 2, paragraph 5.

11.3. On- and Off-Base Ground Movement of Nuclear Weapons. Refer to DoD 5210.41-M in addition to paragraphs 11.3.1 through 11.3.8 of this instruction for personnel, equipment, and procedures to use during logistic ground movements of nuclear weapons outside a restricted area. **EXCEPTION:** These standards don't apply to tactical movement of nuclear weapons.
11.3.1. Security Force Requirements. See AFI 31-101 Volume 2, paragraph 5.2.1.
11.3.2. Security Force Arming and Equipment. Arm individuals accompanying the convoy with an M16 rifle. You may arm maintenance technicians with a 12-gauge shotgun.
11.3.2.1. MAJCOMs prescribe the weapons mix for the RF supporting the convoy. Base the mix on the local environment, current threat situation, and other relevant factors. See Chapter 6 for mandatory armament and equipment requirements. Ensure each convoy has a public address system.
11.3.3. Convoy Security Procedures. Before a ground convoy starts, sweep the primary and alternate routes for hazards. (A security team preceding a missile convey satisfies this requirement.) Missile convoys may not depart the missile support installations without helicopter escort unless the installation commander, or when delegated, a missile wing or group commander authorizes it.
11.3.4. OCONUS Procedures. In OCONUS areas, theater directives, policies, implementing directives, and international agreements prescribe procedures for coordinating work and establishing liaisons between affected agencies.
11.3.5 Pre-departure Briefings. Each MAJCOM with responsibility for securing nuclear weapons movements must draft a pre-departure guide to brief all participants at the unit level before they move weapons. Include:

11.3.5.1. Destination and weapon type.
11.3.5.2. Primary and alternate routes, and en route safe areas.
11.3.5.3. Use-of-Force rules, local THREATCONs, and vehicle safety precautions.
11.3.5.4. Actions to secure disabled vehicles and defend against attack.
11.3.5.5. Communications procedures.
11.3.5.6. Identification of vouching authority.
11.3.5.7. An equipment check of all participants.

11.4. Nuclear Weapon Storage Areas (WSA). According to DoD 5210.41-M and this instruction, MAJCOMs must develop procedural guidelines for entry control, security force requirements, search procedures, and storage structure openings and closings.
11.4.1. Security Force Requirements. See AFI 31-101 Volume 2, paragraph 5.
11.4.2. Emergency Entry Procedures. See AFI 31-101 Volume 2, paragraph 5.

11.5. Weapons Storage and Security System (WS3). DoD 5210.41-M and this instruction outline the criteria for securing weapons storage vaults (WSV) and HAS for nuclear force generation. Designate areas containing WSVs with weapons in them as restricted areas.
11.5.1. Security Force Requirements. See AFI 31-101 Volume 2, paragraph 5.2.1.
11.5.2. Security Procedures. Lock HASs that contain WSVs. **EXCEPTION:** Don't lock HASs when they are occupied or under observation by authorized personnel.
11.5.3. HQ USAFE Responsibilities. HQ USAFE establishes procedures for vault opening and closings and daily physical security check requirements.
11.5.4. WS3 Universal Release Code (URC) Storage.
11.5.4.1. Security measures will ensure no single individual can access URCs.
11.5.4.2. When present on an installation, URCs will be stored only in an alarmed facility or 24-hour manned facility, with duress capability. The alarm must annunicate at a location separate from where the safe is located. "A" and "B" components will be stored in separate containers.

11.6. Munitions Squadrons (MUNS). See DoD 5210.41-M for guidelines.

11.7. 896 MUNS, Nellis AFB, NV.
11.7.1. Security Force Requirements. See AFI 31-101 Volume 2, paragraph 5.2.1. for security force requirements.
11.7.2. Electric Fence. The civil engineer:
11.7.2.1. Checks electric fences for proper operation every 30 days.
11.7.2.2. Post signs, 1-ft by 2-ft, on the outer legal barrier fence at intervals of no more than 100 ft.
11.7.2.3. Print on each sign, in red lettering on a white background: "WARNING - ELECTRICALLY CHARGED FENCE - HIGH VOLTAGE - WARNING"
11.7.2.4. Paint each sign with a skull and crossbones (illiteracy symbol).
11.7.3. Physical Characteristics. The terrain and physical shape of the area may make it economically unfeasible to level, clear, and completely eliminate vegetation and trees. In such areas, use all available lighting.
11.7.4. IDS Inspections. Security police work jointly with BISS maintenance personnel to inspect exterior IDS every 30 days. Conduct a weekly inspection of 1/4 of the system.
11.7.5. Central Security Control (CSC). The SSCC meets the need for a CSC. Remote IDS is not required.

11.8. 898 MUNS, Kirtland Underground Munitions Storage Complex (KUMSC).
11.8.1. Controlled and Restricted Areas. The Kirtland AFB ISC:
11.8.1.1. Designates the underground portion of the facility a restricted area.
11.8.1.2. Designates the KUMSC topside area a controlled area and marks the legal boundary with a type B fence.
11.8.1.3. Designates as controlled areas:
11.8.1.3.1. The ends of the entry and exit tunnel (that is, the portion outside the bifold doors).
11.8.1.3.2. Enrollment center.
11.8.1.3.3. Armory.
11.8.1.3.4. Utility facility.
11.8.1.3.5. Posts the topside controlled area (fenced area) with bilingual controlled area signs.
11.8.2. IDS Requirements. See AFI 31-101 Volume 2, paragraph 5.
11.8.3. Physical Security Requirements. See AFI 31-101 Volume 2, paragraph 5.

11.8.4. Security Force Requirements. See AFI 31-101 Volume 2, paragraph 5.
11.8.5. Arming Requirements. Arm security personnel on duty inside KUMSC with sidearms and have shotguns readily available. Security force planners may arm personnel posted in the ECP or loading dock with M16s instead of shotguns. Make sure that munitions personnel have M16 rifles readily available when the loading dock contains munitions and during DoD convoy operations.
11.8.6. Security Procedures. See AFI 31-101 Volume 2, paragraph 5.

11.9. Department of Energy (DoE) Material. DoE shipments may include radioactive material, high explosives, or nuclear warheads.
11.9.1. The AF:
11.9.1.1. Assumes security of shipments when AF personnel accept custody.
11.9.1.2. Requires security according to the type of resource contained in the shipment.
11.9.2. Parking Safe Secure Transport (SSTs). Air Force personnel normally direct DoE SST vehicles to park inside a WSA. If a WSA isn't available, park the SST in an established restricted area or establish a temporary restricted area. Provide positive entry control and an RF and BF.
11.9.3. SAFE HAVEN Procedures. DoE personnel seek SAFE HAVEN for many reasons, including:
11.9.3.1. Natural disaster.
11.9.3.2. Civil disorder.
11.9.3.3. Hazardous roads or adverse weather.
11.9.3.4. Security threats.
11.9.3.5. Equipment breakdowns.
11.9.3.6. Installation authorities normally receive advance notice of a DoE request for SAFE HAVEN from the installation command post.
11.9.3.7. The installation command post receives DoE requests through the Joint Nuclear Accident Coordinating Center (JNACC) at Headquarters Defense Nuclear Agency.
11.9.4. Identification for Convoy Personnel. See AFI 31-101 Volume 2, paragraph 5.
11.9.5. Security Support for Scheduled DoE Shipments. The DoE Transportation Management Branch, Albuquerque, NM, notifies the installation in advance of a scheduled DoE shipment. The DoE Transportation Management Branch can answer questions concerning DoE:
11.9.5.1. Courier teams.
11.9.5.2. Equipment.
11.9.5.3. Identification.
11.9.5.4. Shipment arrival times.
11.9.5.5. Vehicle license and ID.
11.9.6. Shipment problems.
11.9.6.1. During duty hours, you may reach the Transportation Management Branch at: DoE Transportation Safeguards Division, commercial (505) 845-6724.
11.9.6.2. During non-duty hours, call: DoE Security Communications Control Center, commercial (505) 845-6952/5291/6656.
11.9.6.3. If you can't make contact with the above numbers, call the JNACC office at DSN 221-2102/2104, commercial (703) 325-2102/2104, or the DoE JNACC office at commercial (505) 845-4667.
11.9.7. Vehicle Sanitation/Inspection. The DoE convoy commander certifies all arriving convoy vehicles as sanitized, under continuous observation following sanitation, and not containing prohibited articles.
11.9.7.1. Allow certified DoE convoy vehicles and personnel to enter or leave the restricted area without inspection.
11.9.8. Inspections. Installation commanders, or when delegated, the group commander responsible for the security of the area may direct inspections of all DoE vehicles entering or leaving restricted areas or no-lone zones and the couriers' personal gear. Empty trailers may be inspected only within restricted areas or no-lone zones. **EXCEPTION:**Security forces may search loaded trailers in limited or exclusion areas with the DoE convoy commander's permission.
11.9.9. Courier Teams. Allow DoE courier team members entering the area to dismount for ID on a rotational basis so they can maintain the DoE level of security for the material in custody. Grant DoE couriers entry as visitors under escort of an AF escort official.
11.9.9.1. The DoE convoy commander must maintain custody and security of the shipment until the AF accepts custody.
11.9.9.2. Only an authorized AF recipient (accountable officer or alternate) may accept custody of DoE material. Ensure the DoE convoy commander and accountable officer verify each other's identity and authorization.

11.9.9.3. Designate the interiors of the transport vehicles as no-lone zones when the courier or maintenance personnel begin sanitizing efforts. They remain a no-lone zone until all critical components are removed. Keep this designation for vehicles waiting to be reloaded with critical components.
11.9.9.4. Air Force personnel must escort the DoE team's entry to restricted areas and no-lone zones. **EXCEPTION:** No-lone zones inside DoE transport vehicles. If hostile action or other emergencies occur while an installation hosts a DoE convoy and DoE has custody of the loaded vehicles, make sure AF SP assist DoE couriers secure the vehicle.
11.9.9.5. The installation commander or on-scene commander must assume overall direction of DoE and AF security forces to ensure they work together efficiently. This direction must not compromise the integrity of loaded vehicles remaining in DoE custody.

11.10. Nuclear Cargo, Limited Life Components (LLC), and Nuclear Support Material. Paragraphs 11.10.1 through 11.10.14.5. give the standards for securing nuclear cargo logistically transported by aircraft between USAF installations and other Government or service installations.

NOTE: The security measures for military aircraft apply to contract air carriers.
11.10.1. Type I Security. See AFI 31-101 Volume 2, paragraph 5.
11.10.2. Type II Security. See AFI 31-101 Volume 2, paragraph 5.
11.10.3. Security Facilities. If possible, park type II aircraft in an existing permanent restricted area containing priority A or B resources. Mark the boundary of a temporary area with an elevated rope and stanchion barrier and post restricted area signs along the boundary and at the ECP. Coordinate with the air crew to determine when the aircraft will be roped. Ropes are not required if the aircrew is present. Identify the ECP and provide lighting to illuminate approaches to the aircraft.
11.10.4. Security Procedures. *MCR 55-18, Operational Procedures for Aircraft Carrying Hazardous Materials*, Oct 93, requires aircrew members notify installation personnel when they're on-loading, off-loading, or en route to an installation. On-load, off-load, or en route notice from aircrew members constitutes notice of security requirements.
11.10.5. Enroute Security Requirements. Organizations responsible for operating missions transporting nuclear cargo and classified nuclear support material, including LLC, must give advance notice of their security requirements to en route installations.
11.10.6. Arrival and Landing. At least one, two-member response team meets the aircraft as it taxis off the runway and follows the aircraft, at a safe distance, to it's parking location. The courier team will not initially deploy outside the aircraft upon arrival. Only an aircrew member and flight engineer or scanner will initially deplane for arrivals. The courrier will deplane after receiving feedback from these individuals.
11.10.6.1. Senior Security Force Supervisor:
11.10.6.1.1. Monitors the arrival of the aircraft.
11.10.6.1.2. Coordinates security procedures with the courier.
11.10.6.1.3. Directs security operations.
11.10.6.1.4. Gives the courier a concise threat assessment and a duress code developed by the SP for the duration of ground time.
11.10.6.2. The aircrew courier will coordinate with the on-scene security representative for required support. If the aircrew courier decides security isn't adequate and the deficiency can't be corrected, the aircraft departs.
11.10.6.3. Off-Load or Enroute Security Procedures. Once the aircrew parks the aircraft and security forces establish security, follow the procedures for off-load and subsequent on-load in paragraph 11.10.10. Continue type I security requirements for aircraft off-loading nuclear cargo until you can provide security for local ground movement in accordance with this instruction.
11.10.7. Type I Entry Control Procedures. The security force must inspect the hand-carried possessions of everyone entering or leaving the area for contraband, such as weapons or explosives. Security force members may inspect aircrew and courier baggage.
11.10.7.1. Munitions and security personnel sanitize vehicles by removing all nonessential personnel and checking for explosive materials.
11.10.7.2. Before loading nuclear cargo on an empty aircraft, the courier ensures all nonessential personnel leave the area and hazardous materials are removed. Use explosive detector dog teams where available.
11.10.7.3. Courier and Security Force Supervisor:
11.10.7.3.1. Give the EC a list of people who may enter the restricted area unescorted.
11.10.7.3.2. Authenticate the list.
11.10.7.4. The CIS identifies people on the list when they enter restricted areas using the USAF RAB.
11.10.7.5. HQ USAFE, in its supplement to this instruction or Allied Command Europe Directive 80-6/EUCOM Directive 60-10, *Nuclear Surety Management*, Nov 87, outlines procedures used at non-US NATO installations.
11.10.7.6. The courier designates escort officials at non-US NATO installations.

11.10.7.7. The courier or designated escort officials must vouch for and sign into the area anyone who isn't authorized unescorted entry at non-US NATO installations.
11.10.8. Crew Rest Security Procedures. The courier must seal all doors and hatches of a nuclear-laden aircraft before they depart.
11.10.8.1 The area security supervisor, accompanied by an aircrew two-man team, must verify the seals numbers, record the crew door seal number and give it to CSC.
11.10.8.2. After the two-man team verifies the seals, the security forces monitor the restricted area and no-lone zone.
11.10.8.3. The aircraft commander or the aircrew courier must inform security controllers at CSC or the installation command post of their location.
11.10.8.4. Permit entry to the restricted area only to an authorized aircrew two-man team.
11.10.8.5. When the aircrew returns to the aircraft, the area supervisor must go with the aircrew two-man team into the area to make sure all seals are intact and the crew door seal number is the same as the one recorded.
11.10.8.6. In an emergency endangering a sealed aircraft, emergency personnel may enter the restricted area and, if necessary, the aircraft. Immediately notify the aircrew courier or aircraft commander.
11.10.9. Convoy Arrival Procedures at the Aircraft. Don't stop the convoy from entering the restricted area to identify convoy personnel. Base the initial entry authority for convoy personnel on the security force supervisor's authentication. Ensure personnel have valid USAF RABs and their names appear on the local entry list. Authenticate the number of people and the validity of their credentials before you leave the storage or staging area. Include the number of vehicles entering the area.
11.10.10. Departure Security Procedures. In the final stages of pre-departure, the flight engineer or scanner maintenance crew chief may work alone outside the aircraft, and will normally be the only person outside during engine start.
11.10.10.1. At least one, two-person patrol must stand by to watch the aircraft. The patrol must follow the aircraft to its assigned runway and stand by until it lifts off. If the aircraft must return, follow arrival and landing security procedures.

NOTE: RF requirements remain in effect during departure and for 30 minutes after the aircraft has departed.
11.10.11. Logistic Aircraft Movement of LLCs, Classified Nuclear Support Material, and Aircraft Sanitized To Carry Nuclear Cargo. After searching and sanitizing an aircraft, maintain entry control. When subsequent missions involve nuclear cargo, you must maintain entry controls even when nuclear cargo, LLCs, or classified nuclear support material are completely downloaded.
11.10.11.1. The aircraft commander or courier may authorize the release of type II security requirements for empty, sanitized aircraft. Resanitize the entire aircraft before on-loading nuclear cargo. If possible, park the aircraft in an existing restricted area containing priority A or B resources. If this isn't possible, park the aircraft in the most secure area available and establish a temporary restricted area.
11.10.11.2. The aircrew must secure the cargo when they are at the aircraft. Ropes are not required if the aircrew is present at the aircraft.
11.10.11.3. If the aircrew must leave the aircraft, download LLCs and classified nuclear support cargo and place them in the most secure storage available. If downloading is impracticable, post one security force member at the aircraft to enforce entry control. Seal the aircraft.
11.10.11.4. The security force supervisor must verify the seals and relay the seal numbers to security controllers at CSC.
11.10.11.5. The aircraft commander or the aircrew courier must inform security controllers or the installation command post of their location.
11.10.11.6. In an emergency endangering the aircraft, emergency personnel may enter. Immediately notify the aircrew courier or aircraft commander.
Reestablish the integrity of the area once the situation is rectified. Station a SRT or ART close by to react to security incidents.

Chapter 12

STANDARD FOR PRIORITY A AIRCRAFT

12.1. Overview. This chapter prescribes the priority, security force, physical security requirements, and special procedures for securing priority A aircraft. Chapters 6, 7, & 8, of this instruction, levy other physical security program requirements. (See other chapters of this instruction for logistic aircraft movements of nuclear cargo and Presidential support aircraft.)

12.2. Priority A. Use priority A for:
12.2.1. Nuclear-loaded bomber and fighter aircraft.

12.2.2. Alert National Airborne Operations Centers (NAOC) (E-4s-formerly National Emergency Airborne Command Post (NEACP)).
12.2.3. Alert Take Charge and Move Out (TACAMO) relay aircraft.
12.2.4. Alert ACC post attack command and control system (PACCS) EC-135.

NOTE: PACCS include Commander-in-Chief USSTRATCOM Airborne Command Post, auxiliary command post, airborne LCC, and radio-relay aircraft.

NOTE: "Alert" is defined as aircraft EWO configured, crew assigned, and in an alert posture, i.e., crew activities limited to meet near immediate, timed, response criteria.

12.3. Security Requirements for Nuclear-Loaded Aircraft.
12.3.1. Security Force Requirements. See AFI 31-101 Volume 2, paragraph 6.
12.3.2. Two Person Policy. Before the introduction of nuclear weapons, sanitize the aircraft of unauthorized personnel and post a CIS and CBS. After completing up-load operations, you may remove the CBS if you can still comply with the two-person policy and maintain boundary surveillance.
Provide patrol surveillance for nuclear-loaded aircraft towed or taxied within or between restricted areas. Comply with DoD 5210.41-M regarding search procedures.
12.3.3. Circulation Control. MAJCOMs develop or approve specific circulation controls for restricted areas containing nuclear-loaded aircraft. These must be published in MAJCOM or installation directives.

12.4. Priority A Nonnuclear Aircraft.
12.4.1. Physical Security Requirements. Provide the physical security aids outlined in this instruction to parking areas.
12.4.1.1. Positive entry control for the restricted area and individual aircraft.
12.4.1.2. Continuous boundary detection and assessment capability of the entire boundary and aircraft.
12.4.2. Security Force Requirements. Provide:
12.4.2.1. Security forces to maintain enforcement of the two-person rule if Two-Person Control (TPC) material is onboard the aircraft and when TPC material cannot be removed. See paragraph 1.18.4.
12.4.2.2. At least one armed security force member dedicated for response to the aircraft.
12.4.2.3. At least one other armed security force member dedicated to the restricted area.
12.4.2.4. An external armed response team (normally an SRT) available to respond within 5 minutes to any aircraft's location.

NOTE: Security force of 3-5 people available to respond within 5 minutes. (May include mobile security force members posted at or within the restricted area, and the SRT.)

12.5. Alert Crews and Alert Crew Billets: Alert crews and billets are not designated a security priority.
12.5.1. During peacetime, prudent physical security measures should be applied to alert crew billets such as keeping windows locked, installing cipher locks on the doors, and conducting periodic security checks, etc.
12.5.2. During periods of strategic warning, local plans should identify appropriate security enhancements and procedures.

Chapter 13

STANDARD FOR PRIORITY B AIRCRAFT

13.1. Overview. This chapter prescribes requirements for securing priority B fighter, air refueling, bomber, airlift, air support, command and control, and reconnaissance aircraft parked in mass or dispersed aircraft areas. Chapters 6, 7, & 8, of this instruction, levy other physical security program requirements. Use the SSS for priority A or C aircraft when priorities change due to mission requirements.

13.2. Security Priorities. Designate priority B during peacetime for:
13.2.1. Alert (conventional) aircraft (i.e., fighter, bomber, special operations, reconnaissance, air support, and air refueling aircraft.)
13.2.2. F-117A aircraft when away from home stations.
13.2.3. All airborne warning and control system aircraft.
13.2.4. U-2R aircraft. **EXCEPTION:** Those stationed in CONUS, Alaska, and Hawaii.

13.2.5. Back-up alert CINCLANTCOM, CINCPACOM, CINCEUCOM, PACCS (see **NOTE** in para 12.2.), EC-135, and TACAMO aircraft when preflight and maintenance ready, PACCS radio relay, and off-alert NAOC E-4 aircraft.
13.2.6. RC-135s. At contractor facilities these must receive the same level of security required for priority B resources under AF control.
13.2.7. SR-71 aircraft while OCONUS. (See Chapter 14 for CONUS, Alaska, Hawaii & Guam requirements.)
13.2.8. Any Special Operations Forces (SOF) aircraft permanently or temporarily Sensitive Compartmented Information (SCI) configured and C-130s permanently configured for airborne reconnaissance missions or carrying pallets (COMFY LEVI and SENIOR SCOUT), vans, or containers for SCI operations. Designation of SCI/mission configuration should be determined by the local commander or aircraft commander NLT 24 hours prior to the requirement for priority B security.
13.2.9. Alert Compass Call Aircraft, and B2 Bombers.

NOTE: B-2 bombers maintain their security priority while in depot maintenance).

13.3. Security Force Requirements. For priority B aircraft, provide:
13.3.1. Positive entry control for the restricted area containing the aircraft.
13.3.2. Surveillance and intrusion detection at the restricted area boundary and the resource(s).
13.3.3. At least one armed security force member dedicated for immediate internal armed response.
13.3.4. External armed response (normally an SRT) available to respond within 5 minutes to any aircraft's location.

13.4. Aircraft Away from Home Station. MAJCOMs must approve the use of host security forces (US or foreign), military and civil police, or other DoD personnel to provide response capability for aircraft deployed from home stations.

13.5. F-117A on Static Display. Post one security force member with an M16 at the front and rear of the aircraft. You may post additional sentries based on local conditions. You must provide a two-person armed response. The aircraft is touch sensitive; therefore, while on static display, errect a barrier a minimum of 20 feet from the aircraft.

13.6. Deployed SOF Aircraft. Special mission aircraft standards apply to COMFY LEVI and SENIOR SCOUT missions. Strive for the same level of security at home-station and deployment locations.

13.7. Tailored Security. Standard physical security measures (see Chapters 6, 7, and 8) may be impractical at times due to mission, terrain, climate, sociopolitical sensitivities, or other factors. At deployment locations, tailor security measures to meet unique requirements. For example, some countries don't allow armed security personnel. On other deployments, the mission may rely on maintaining a low profile and attracting as little attention as possible. See Joint Service Regulation AR 190-16/AFR 207-4/OPNAVINST 5530.15/MCO 5500.13A/DLAR 5710.4, *Physical Security*, for security requirements for locations controlled by other military services. Lock and sensor aircraft entry points and hatches.

13.8. Special Security Procedures.
13.8.1. Conventional Alert and Air Refueling Alert Aircraft. MAJCOMs must develop entry control procedures for aircraft maintained on alert status in permanent or dispersal areas.
13.8.2. SCI Configured Aircraft.
13.8.2.1. Secure all hatches to prevent undetected entry to the aircraft. Equip hatches that cannot be secured with numbered seals.
13.8.2.2. The maintenance supervisor or aircrew installs the seals and provides the seal numbers to the security force.
13.8.2.3. The security force periodically checks the seals.
13.8.2.4. Lock and seal SCI mission aircraft accredited as an airborne special compartmented information facility (SCIF) when unattended. Personnel locking and sealing or opening accredited aircraft must have authorized SCI access. Accredited SCIF mission aircraft require an EAL when parked in a restricted area. SCI mission aircraft without airborne SCIF accreditation require an EAL only when parked in temporary restricted areas.
13.8.2.5. The aircraft commander or maintenance supervisor provides the security force with the EAL for authentication. Normally, remove SCI material from the aircraft when personnel complete a mission or at unscheduled stops. When you can't remove SCI material or when suitable storage locations aren't available, ensure SCI-indoctrinated personnel remain with the aircraft and control entry into the SCI compartment. If the aircraft has to make an unscheduled landing, provide security support.
13.8.2.6. For unscheduled landings at non-USAF installations, the maintenance supervisor must control entry and maintain surveillance of the aircraft.

Chapter 14

STANDARD FOR PRIORITY C AIRCRAFT

14.1. Overview. This chapter prescribes the priority, security force, physical security requirements, and special procedures that you must use to secure priority C aircraft. Chapter 6,7, & 8, this instruction, levy other physical security program requirements. Use other SSSs specified in this instruction for securing aircraft upgraded to priority A and B.

14.2. Security Priorities. These aircraft are priority C during peacetime configuration:
14.2.1. Non-alert air support, fighter, and air refueling, aircraft.
14.2.2. Non-alert F-117A aircraft when at home and at depot maintenance.
14.2.3. U2R aircraft in CONUS, Alaska, and Hawaii.
14.2.4. USAFE dual-capable aircraft.
14.2.5. Non-alert PACCS, TACAMO, and EC-135 aircraft.
14.2.6. Airlift and Civil Reserve air fleet aircraft.
14.2.7. SR-71 aircraft while in CONUS, Alaska, Hawaii, & Guam.
14.2.8. SOF aircraft when they aren't configured as special-mission aircraft during COMFY LEVI and SENIOR SCOUT missions.
14.2.9. E-4, TACAMO, and EC-135 aircraft undergoing contract maintenance at civilian contractor facilities.

NOTE: The AF doesn't assign these aircraft a security priority but contractors ensure they receive security support commensurate with priority C standards.
14.2.10. Alert helicopters specifically support NAOC operations.
14.2.11. Non-alert bomber aircraft (except B-2s) and bomber aircraft supporting conventional combat operations.
14.2.12. RC-135 aircraft, unless SCI-configured.
14.2.13. HC-130 rescue aircraft.
14.2.14. Non-alert Compass Call aircraft.

14.3. Security Force Requirements for Mass/Dispersed Aircraft Parking Areas. Owner and user personnel provide surveillance for aircraft parking areas. Security forces provide:
14.3.1. An ART dedicated to the restricted area to assist support personnel in observing area boundaries and responding to alarms.
14.3.2. An additional armed response force of at least 2 people (usually an SRT or LE) available within 5 minutes of an alarm.
14.3.3. Provide equivalent security to aircraft deployed off the installation.
14.3.4. Assign additional forces based on the threat, the geographical location, and other factors.
14.3.5. Joint regulation AR 190-16/AFR 207-4/OPNAVINST 55-30.15/MCO 5500.13/DLAR 5710.4 outlines aircraft security requirements for other military services.

14.4. Physical Security Requirements. Parking areas require the physical security aids outlined in Chapters 7 and 8 of this instruction.
14.4.1. Securing SOF Aircraft. Lock and sensor all SOF aircraft entry points and hatches. Adapt this instruction's other standard security measures to whatever extent the mission, terrain, climate, and socio-cultural circumstances allow. At deployed locations, tailor the security measures to meet the requirements of host countries (for example, some countries don't permit armed security personnel).
14.4.2. Supporting Force Responsibilities. MAJCOMs prescribe supporting force responsibilities and entry control procedures for restricted areas containing priority C resources.
14.4.3. NAOC Helicopter Support. Owner and user personnel may control entry to the aircraft, alert hangars, and crew billets.

Chapter 15

STANDARD FOR PRESIDENTIAL, SENIOR EXECUTIVE MISSION, SPECIFICALLY DESIGNATED SPECIAL AIR MISSION, AND SPECIAL AIR MISSION AIRCRAFT

15.1. Overview. This chapter prescribes priorities, minimum security force requirements, physical security, and special procedures for Presidential, SENEX Mission, SDSAM, and SAM aircraft.

15.2. Security Priorities. Security priorities are assigned in accordance with Figure 15.1.

Figure 15.1. Security Priorities for Presidential, Senior Executive Mission, Specifically Designated Special Air Mission, and Special Mission Aircraft.

Restricted Areas Containing These Types of Facilities and Equipment:	Security Priority
Presidential and SENEX aircraft retain their priority regardless of operational status or location, including depot maintenance.	A
SAM aircraft assigned a mission designated as SDSAM status will be upgraded to priority A status after a joint sweep is conducted by the assigned aircraft security NCOs and Flight Engineers/Flight Mechanics 2 hours prior to departure. These aircraft will retain their priority A status until mission completion.	A
Fuel designated for use on Presidential aircraft is priority A from the time the sample is taken for analysis until it is put in the aircraft.	A
VC-137 aircraft unless upgraded to Presidential or SDSAM status and designated VC-9 aircraft.	B
C-9C, C-20B aircraft unless upgraded to Presidential or SDSAM status.	C

NOTE: Refer to paragraphs 1.3.2., 1.4.2., and 1.5.2. for general entry control, boundary detection and surveillance, and RF security requirements. Chapters 7 and 8 provide general physical security and IDS requirements. Refer to paragraphs 15.4. through 15.8. for specific requirements.

15.3. Responsibilities for Physical Security. The Chief, Presidential Aircraft Security, directly supervises Presidential aircraft security.

15.3.1. Aircraft commanders ensure security arrangements are adequate while away from home station. Aircraft commanders ensure security arrangements, i.e. point vehicle (regardless of the location or duration of ground time), lights, ropes and stanchions are arranged in advance and adequate while away from home station.

15.3.2. Installation commanders provide security forces, equipment and facilities for Presidential aircraft, as requested by the Director of the White House Military Office, the HQ USAF Presidential Project Officer (or the officer's advance agents), or the US Secret Service.

15.4. Security for Presidential Aircraft.

15.4.1. Entry Control Requirements. Establish entry control procedures IAW paragraph 12.4.1. of this instruction. HQ Air Mobility Command (HQ AMC), in conjunction with the White House Military Office and the US Secret Service, must establish detailed procedures for allowing aircraft access to unescorted and escorted individuals. HQ AMC must provide this information to passengers, home stations, and deployed agencies as necessary.

15.4.2. Fuel Security and Analysis. HQ AMC must outline specific procedures for analyzing fuel on Presidential aircraft and distribute the regulations to supporting units.

15.4.2.1. Fuels personnel and/or Air Force One advance agents take test samples from the fuel source utilizing prescribed procedures of AFM 67-1, Vol 1. Air Force One advance agents provide the seals and are responsible for ensuring they are attached to the vehicle containing the tested fuel and arrange for security of the designated fuel trucks until delivery to Air Force One. Fuel trucks designated for Presidential usage may be parking in existing Priority A security areas. Personnel at home station responsible for providing, analyzing, or securing fuel designated for Presidential Aircraft must meet the requirements of DoD Directive 5210.55 (Selection of DoD Military and Civilian Personnel and Contractor Employees for Assignment to Presidential Support Activities) and AFI 35-501)Personnel Security Program Management). These personnel who have regular and frequent contact with or access to Presidential facilities must be the subject of a Special Background Investigation. Aircraft Commander may waive or modify requirements based on mission needs.

15.4.3. Aerospace Ground Equipment (AGE) Systems Security. Inspect and place AGE in a restricted area or keep it under constant surveillance. Inspect the equipment with an explosives detection dog team or qualified Explosive Ordinance Disposal (EOD) team before using it.

15.4.4. Baggage and Cargo Security. The aircraft commander approves all aircraft cargo, except for the personal baggage of crew members and passengers.
15.4.4.1. The US Secret Service representative inspects and approves all personal and hand-carried articles of passengers before loading.
15.4.5. Security for Aircraft Arrival and Departure. Air Force security forces maintain security responsibilities for controlling entry to the aircraft during all facets of the Presidential flight. Security forces coordinate security activities with US Secret Service personnel.
15.4.5.1. The home station and those installations that expect to frequently support Presidential aircraft deployments must publish a plan or annex to the local security plan outlining support requirements. The plan must include:
15.4.5.1.1. Detailed figures on the installation's committed security forces.
15.4.5.1.2. Responsibilities for controlling aircraft access and crowds.
15.4.5.1.3. Roles of OSI agents.
15.4.5.1.4. Guidelines for explosive ordinance disposal support, security communications, and other appropriate support equipment requirements.
15.4.5.2. Close on-base perimeter roads to vehicular/pedestrian traffic to secure the base for Presidential aircraft. The US Secret Service approves exceptions. Ask military or civilian police authorities to provide rescue capability and control of boat traffic when flight plans call for the aircraft to arrive and depart at a low level over water.
15.4.6. Security Requirements for Home Station. In addition to the requirements in Chapters 7 and 8 of this instruction, provide a hangar for sole use of the aircraft and support equipment.
15.4.6.1. HQ AMC must identify additional security requirements and equipment if the aircraft is parked outside the established restricted area.
At home stations for Presidential Aircraft:
15.4.6.1.1. One close-in sentry for each aircraft.
15.4.6.1.2. One close boundary sentry for each aircraft located outside the Presidential Exclusive Parking Zone (PEPZ). A close boundary sentry is not required for aircraft parked within the PEPZ or within the Air Force one Maintenance and Support Complex.
15.4.6.1.3. Close boundary sentries (3) to provide immediate visual assessment if the BISS alarm system is inoperative at the Air Force One maintenance and Support Complex.
15.4.6.1.4. Security Response Team capable of responding within five minutes.
15.4.6.1.5. Entry Controller at all designated vehicle and personnel entry points at the Air Force One Maintenance and Support Complex.
15.4.6.1.6. Ropes, stanchions, restricted area signs and light-all units will be provided if aircraft has to be parked outside the Air Force One Maintenance and Support Complex.
15.4.7. Minimum Security Force Requirements for the Home Station. The 89th Security Police Squadron must provide:
15.4.7.1. Aircraft supervision.
15.4.7.2. Close-in security for each aircraft.
15.4.7.3. Boundary surveillance for VC-137 and C-25A aircraft and each aircraft located outside the dedicated hangar.
15.4.7.4. Entry controls to the aircraft hangar parking area.

NOTE: This security requirement may encompass boundary surveillance duties.
15.4.7.5. Dedicated internal response.
15.4.7.6. External response within 5 minutes.
15.4.8. Security Requirements Off Home Station. Presidential support deployed personnel provide entry control and supervision. At U.S. military installations support needs are as a minimum:
15.4.8.1. A temporary restricted area for each aircraft.
15.4.8.2. A designated entry control point to the aircraft.
15.4.8.3. A hangar, if available.
15.4.8.4. A temporary restricted area for the Presidential aircraft fuel supply if space in existing restricted areas is unavailable.
15.4.8.5. A portable intra-base radio for the entry controller and each host security force member providing direct support.
15.4.8.6. A sidearm for each close boundary sentry.
15.4.8.7. A vehicle or sentry shelter for each entry controller.
15.4.8.8. Enough rope, stanchions, and restricted area signs to establish close-in security and temporary restricted areas for each aircraft.
15.4.8.9. Four light-all units for each aircraft and two light-all units for the Presidential fuel supply.
15.4.8.10. A two person security response team capable of responding within five minutes.
15.4.8.11. The host unit provides boundary surveillance, external response within 5 minutes, and fuel security. Boundary surveillance will consist of two boundary guards who will remain mobile at the rear of the aircraft.

15.5. Security for SENEX Mission Aircraft.

15.5.1. Entry Control Requirements. HQ AMC must establish entry control requirements.

15.5.2. Fuel Selection and Analysis. Make a laboratory analysis of the aircraft fuel when the mission directly supports the President or as other circumstances warrant. Follow the procedures in Paragraph 15.4.2.

15.5.3. AGE Security. Follow the procedures in Paragraph 15.4.3.

15.5.4. Baggage and Cargo Security. The aircraft commander approves all cargo and non-personal crew baggage before loading.

15.5.4.1. Crew members must protect their personal baggage.

15.5.4.2. Security force personnel inspect crew members and personal baggage if no antihijack screening procedures are in place.

15.5.5. Aircraft Arrival and Departure. Security Personnel will always accompany SENEX aircraft regardless of the length of the mission.

15.5.6. Security Requirements at Home Station. Follow the procedures in Paragraph 15.4.6.

15.5.7. Manning Standards at Home Station. Security personnel must provide:

15.5.7.1. Aircraft supervision.

15.5.7.2. Close-in security for all aircraft when located inside or out of the designated hangar.

15.5.7.3. Internal response.

15.5.7.4. Entry controls.

15.5.7.5. External response within 5 minutes.

15.5.8. Security Off Home Station. Park and secure the aircraft in a hangar if available. Provide lighting.

15.5.8.1. The home station security personnel provide security supervision and entry control.

15.5.8.2. The host unit must provide boundary surveillance when requested by the aircraft commander. The host unit must also provide external response within 5 minutes or ensure that the host nation can meet the requirement.

15.6. Security for SDSAM Aircraft. Visually inspect AGE equipment before allowing entry to the aircraft restricted area. SDSAM aircraft entry control requirements, fuel selection and analysis regulations, and baggage and cargo security are the same as for SENEX mission aircraft (Paragraph 15.5).

15.6.1. HQ AMC or the aircraft commander must notify the host unit about specific security requirements for aircraft arrival and departure. While off the home station, the home station aircraft security personnel will accompany the aircraft to provide entry control and supervision. Host unit will provide boundary surveillance, and external response within 5 minutes.

15.7. Security for SAM Aircraft. Visually inspect AGE equipment before allowing entry to the aircraft restricted area. **EXCEPTION:** Priority C SAM aircraft. Provide supervision, entry control, an external response within 5 minutes, and a dedicated patrol response for the aircraft parking area at the home station. While off the home station, the aircraft crew members will provide security and entry control during short stops unless home station aircraft security NCOs are assigned to the mission. If the aircraft remains on base for extended periods, provide entry control (unless home station aircraft security NCOs accompany the mission) and external response within 5 minutes.

15.8. Security for Presidential and SENEX Aircraft in Contractor Maintenance Facilities. HQ AMC must augment the requirements in Paragraph 2.1.1 by developing and approving civilian contract maintenance security procedures in accordance DoD 5220.22-M, *Industrial Security Manual for Safeguarding Classified Information*, Jan 91, and AFI 31-701.

15.9. Photographs of Presidential Aircraft. Exterior photographs of the aircraft are permitted when it is parked outside of the Presidential Exclusive Parking Zone (PEPZ). Interior photographs of the Presidential aircraft suite and office are prohibited without the permission of the Director of the White House Military Office. The Presidential Pilot must authorize any photographs of the remainder of the interior of the aircraft including the conference room. Crew members must take proper precautions to prevent the inadvertent release of classified materials or information if photographs are taken.

15.10. Security Exercises and Tests. Exercises or tests of physical security procedures will not be conducted while Presidential Aircraft are temporarily located on an installation. If an actual emergency arises on an installation where Presidential Aircraft are located, a senior representative of the host security agency will report the incident to the Presidential Aircraft Security Officer on duty.

15.10.1. At home station, physical security exercises will not be conducted 2 hours before a Presidential mission arrival or departure. Also, at no time will physical security exercises be conducted in or around facilities or areas that house Presidential Aircraft.

Chapter 16

STANDARD FOR SENSITIVE COMPARTMENTED INFORMATION (SCI) PRODUCTION SYSTEMS

16.1. Overview. This chapter prescribes the priorities, minimum security forces, physical security, and special procedures for securing SCIF and intelligence production systems that the AF designates as priority resources. Implement these measures to deter SCI espionage and exploitation.

16.2. Responsibilities. HQ Air Intelligence Agency's 497 IG/INS:

16.2.1. Oversees the security of all SCIFs.

16.2.2. Coordinates with HQ USAF/SP to resolve conflicts between this instruction and other directives.

16.2.3. Approves additional requirements. (For example: manpower and physical security aids, proposed and funded by operating commands.)

NOTE: Security planners must use this instruction along with Director of Central Intelligence Directive (DCID) 1/21, *Manual for Physical Security Standards for SCIFs*, Jan 94.

16.3. Security Standards. Protect restricted areas containing SCIFs and intelligence production systems by following the procedures in this chapter unless the local senior intelligence official, SP, and AFOSI recommend exceptions after making a risk assessment based on inputs.

16.3.1. The owning-command SP and IN proposes lesser or more stringent security standards and rationale on a case-by-case basis to HQ USAF SP and IN for approval.

16.4. Security Priority, Entry Control, Boundary Surveillance, and RF Support Requirements. Security priorities and security requirements are specified in figure 16.1.

Figure 16.1. Security Priority and Requirements for SCI Systems.

Restricted Areas Containing These Types of Facilities:	Security Priority	Entry [1] Control	Boundary [2] Surveillance	RF [3] Support
Fixed sites engaged in live signals collection.	A	X	X	X
Ground sites that initially process or analyze recorded signals	B	X	X	X
Tactical collection resources when deployed and OCONUS	B	X	X	X
Operational emergency reaction special security offices at a deployed location	B	X	X	X
Training facilities that teach complete mission activities; distribute information on collecting, analyzing, and processing intelligence; and process intelligence data collected by airborne or overhead platforms *NOTE:* Only during collection activitiy.	B	X	X	X
Headquarters, Air Intelligence Agency.	B	X	X	X
Tactical collection resources and emergency reaction special security offices in storage or transit located OCONUS, Alaska, or Hawaii	C	X		X
Other tactical resources where personnel prepare intelligence recording materials when set up and operational.	C	X		X
Primary atennas, beam-forming buildings, and associated signal transmission cables located in CONUS, Alaska, or Hawaii.	C			X
Backup antenna systems located OCONUS, Alaska, or Hawaii.	C			X
NOTE: 497 IG/INS established protection requirements for SCIFs not designated priority resources				

NOTES:

1. An armed person (SCI indoctrinated) controls entry to the SCIF IAW DCID 1/21, para 7-9. Security forces control entry to the restricted area containing the resources.
2. See paragraphs 1.3.2., 1.4.2., and 1.5.2. for examples of boundary surveillance.
3. See paragraphs 1.3.2., 1.4.2., and 1.5.2. for ART and SRT requirements.

16.5. IDS.

16.5.1. Interior Systems. DCID 1/21 prescribes the requirements for SCIF IDS.

16.5.1.1. The resource's senior intelligence officer exclusively oversees SCIF IDS operation and testing.

16.5.1.2. 497 IG/INS must approve SCIF IDS.

16.5.2. Exterior Systems. The resource owner SP in coordination with the hosting MAJCOM SP selects restricted area boundary IDS that minimizes interference with intelligence production.

16.5.3. Beam-Forming Buildings. All doors and any other openings in excess of 96 square inches must have alarms.

16.6. Security Procedures.

16.6.1. Circulation Control. The resource's senior intelligence officer has exclusive authority to grant entry to restricted areas that contain intelligence production system priority resources. Don't authorize prepositioned EALs for inspector generals or hosting MAJCOM officials.

16.6.1.1. The priority resource owner may specify the entry or ID credentials to be used to enter restricted areas containing intelligence production systems.

16.6.2 Convoys. The owning command determines the procedures and equipment for security convoys that have intelligence production resources. Incorporate these instructions in the master security deployment plan as approved by 497 IG/INS.

16.7. Classification. USAFINTEL 201-1 classifies the association of signals intelligence collection and a specific location as "Confidential."

16.8. Forms Prescribed:
16.8.1. AF Form 116, **Request for Deviation from Security Criteria.**
16.8.2. AF Form 213, **Receipt for Accountable Form.**
16.8.3. AF Form 335, **Issuance Record-Accountability Identification Card.**
16.8.4. AF Form 340, **Sensor Alarm Data.**
16.8.5. AF Form 1109, **Visitor Register Log.**
16.8.6. AF Form 1199, CD, **Air Force Entry Control Card (Blue).**
16.8.7. AF Form 1199, CS, **USAF Restricted Area Badge (Blue).**
16.8.8. AF Form 1199-1, **USAF Entry Control Credential Front Label.**
16.8.9. AF Form 1199-2, **USAF Entry Control Credential Pressure Sensitive Label.**
16.8.10. AF Form 1199A, **USAF Restricted Area Badge (Green).**
16.8.11. AF Form 1199B, **USAF Restricted Area Badge (Pink).**
16.8.12. AF Form 1199C, **USAF Restricted Area Badge (Yellow).**
16.8.13. AF Form 2586 (EF), **Unescorted Entry Authorization Certificate.**

RICHARD A. COLEMAN, Colonel, USAF
Chief of Security Police

GLOSSARY OF REFERENCES, ABBREVIATIONS, AND ACRONYMS

References

Internal Security Act of 1950 (50 U.S.C. 797)
Federal Communications Commission Rules and Regulations, Title 47, Part 90, *Private Land Mobile---Radio Services*, Oct 93
Allied Command Europe Directive 80-6/European Command Directive 60-10, *Nuclear Surety Management*, Nov 87
DoDD 3150.3, *Nuclear Force Security and Survivability (S2)*, 16 Aug 94
DoD 5200.1-R, *Information Security Program Regulation*, Jun 86
DoDD 5200.8, *Security of DoD Installations and Resources*, 25 Apr 91
DoD 5210.41-M, *Nuclear Weapon Security Manual*, Apr 94
DoDD 5210.83, *Department of Defense Unclassified Controlled Nuclear Information*,15 Nov 91
DoD 5220.22-R, *Industrial Security Regulation*, Dec 85
DoD 5220.22-M, *Industrial Security Manual for Safeguarding Classified Information*, Jan 91
DCID 1/21, *Manual for Physical Security Standards for SCIFs*, Jan 94
Joint Pub 1-04, *Joint Policy and Procedures Governing Positive Control Material and Devices*, Mar 89.
MCM-179-91, *Chairman's Memorandum CJCS Recovery Plans*
MCR 55-18, *Operational Procedures for Aircraft Carrying Hazardous Materials*, Oct 93
MIL STD 21313G, *Pad Lock Sets - Individually Keyed and Keyed Alike*, 10 Jul 92
MIL STD 35647E, *Pad Lock, Key Operated*, 29 Jul 92
AFR 12-50, Vol 1, *Disposition of Air Force Documentation - Polices, Procedures, and Responsibilities*
AFI 21-204, *Nuclear Weapons Procedures*
AFC 21-209, *Ground Munitions*.
AFPD 31-1, *Physical Security*
AFI 31-101, Volume II, *The Air Force Nuclear Security Program Standards*
AFH 31-103, *Physical Security Handbook*
AFI 31-209, *Air Force Resource Protection Program*
AFI 31-401, *Information Security Program Regulation*
AFI 31-501, *Personnel Security*
AFI 31-601, *Industrial Security Program Management*
AFPD 31-7, *Acquisition Security*
AFI 31-701, *Program Protection Planning*
AFI 31-702, *Systems Security Engineering*
AFI 31-703, *Product Security*
AFH 32-1064, *Standard Facility Handbook*
AFI 36-2104, *Nuclear Weapons Personnel Reliability Program*
AFI 37-133, Vol 1, See AFR 12-50, Vol 1 Above
AFI 91-101, *Air Force Nuclear Weapons Surety Program*
AFVA 125-13, *Military Working Dog Notice*
AFI 190-1, *Inspector General Activities*
AFVA 31-101, *Restricted Area Sign*
AFR 207-4, *Physical Security*
USAFINTEL 201-1, *Security, Use, and Dissemination of SCI*
T.O. 00-35D-54, *USAF Deficiency Reporting and Investigating System*
T.O. 11N-45-51A, *Transportation of Nuclear Weapons Material*
RCS: HAF-XOO(AR)7118, *OPREP 3--Operational Event and Incident Report*
RCS: HAF-SPO(SA)9221, *Physical Security Deficiencies Report*
RCS: HAF-SPO(AR)9346, *Intrusion Detection Equipment Performance Report*
RCS: HAF-SPO(AR)9347, *Sensor Vulnerability Report*
St Athas Pamphlet, *Guidelines for Application of Security Hardware Relating to Bunkers,.Igloos,Huts, and* 01760.

Abbreviations and Acronyms

AF−Air Force
AECS−Advanced Entry Control System
AFB−Air Force Base

AFI−Air Force Instruction
AFOSC−Air Force Operations Support Center
AFOSI−Air Force Office of Special Investigations
AFPD−Air Force Policy Directive
AFR−Air Force Regulation
AFS−Air Force Station
AFSPA−Air Force Security Police Agency
AFT−Alert Fire Team
AFTO−Air Force Technical Order
AFVA−Air Force Visual Aid
AGE−Aerospace Ground Equipment
AMC−Air Mobility Command
ARC−Air Reserve Component
ART−Alarm Response Team
ART-ENL−Air Reserve Technician-Enlisted
ART-OFF−Air Reserve Technician-Officer
AS−Air Station
BF−Backup Force
BISS−Base and Installation and Security System
BMS−Balanced Magnetic Switch
C2−Command and Control
C3−Command, Control, and Communications
C4−Command, Control, Communications, and Computers
CBS−Close Boundary Sentry
CCTV−Closed-Circuit Television
CID−Commercial Item Description
CIS−Close-in Sentry
CIV−Civilian
CONUS−Continental United States
CPU−Central Processing Unit
CSC −Central Security Control
CSP−Chief of Security Police
DCID−Director of Central Intelligence Directive
DES−Data Encryption Standard
DMSP−Defense Meteorological Satellite Program
DNA−Defense Nuclear Agency
DoD−Department of Defense
DoDD−DoD Directive
DoE−Department of Energy
DSCS−Defense Satellite Communication System
DSP−Defense Support Program
DT&E−Developmental Test and Evaluation
EAL−Entry Authority List
EC−Entry Controller
ECF−Entry Control Facility
ECP−Entry Control Point
ENL−Enlisted
FCDNA−Field Command Defense Nuclear Agency
FoF−Force-On-Force
FSC−Flight Security Controller
FT−Fire Team
GPS−Global Positioning System
HAS−Hardened Aircraft Shelter
HHA−Hand-held Annunciator
HHM−Hand-held Monitors
IAR−Invalid Alarm Rate

ID−Identification
IDS−Intrusion Detection Systems
IN−Intelligence Experts
ISC−Installation Security Council
ISP−Installation Security Plan
IVA−Immediate Visual Assessment
JNACC−Joint Nuclear Accident Coordinating Center
KUMSC−Kirtland Underground Munitions Storage Complex
LCC−Launch Control Center
LE−Law Enforcement
LED−Law Enforcement Desk
LF−Launch Facility
LLC−Limited Life Components
LMR−Land Mobile Radio
MAF−Missile Alert Facility
MAJCOM−Major Command
MFT−Mobile Fire Team
MIL−Military
Minimize−A condition when message traffice has been restricted to a location.
MSC−Missile Security Control
MSCF−Master Surveillance Control Facility
MSCFO−Master Surveillance Control Facility Operator
MUNS−Munitions Squadrons
NAF−Numbered Air Force
NAOC−National Airborne Operations Center
NATO−North Atlantic Treaty Organization
NCO−Noncommissioned Officer
NDA−National Defense Area
NSN−National Stock Number
NSNF−Nonstrategic Nuclear Forces
OCONUS−Outside of Continental United States
OFF−Officer
OGS−Overseas Ground Station
OPLAN−Operation Plan
OPR−Office of Primary Responsibility
ORD−Operational Requirements Document
OSI−Office of Special Investigations
OT&E−Operational Test and Evaluation
P3I−Pre-planned Product Improvement
PACCS−Post Attack Command and Control System
PASS−Passive Space Surveillance Operations Center
PCA−Probability of Correct Annunciation
Pd−Probability of Detection
PIN−Personal Identification Number
PPP−Program Protection Planning
PRP−Personnel Reliability Program
PSO−Program Security Office
RAB−Restricted Area Badge
RCS−Report Control Symbol
RF−Response Force
ROCC−Regional Operations Control Center
RS−Reentry System
RTS−Remote Tracking Station
RV−Reentry Vehicle
S2−Survivability and Security
SAM−Special Air Mission

SCC−Security Control Center
SCI−Sensitive Compartmented Information
SCIF−Sensitive Compartmented Information Facility
SDSAM−Specifically Designated Special Air Mission Aircraft
SENEX−Senior Executive Mission Aircraft
SLS−Space Launch System
SOF−Special Operations Forces
SP−Security Police
SRT−Security Response Team
SSCC−Site Security Control Center
SSN−Social Security Number
SSS−System Security Standard
SST−Safe Secure Transport
STD−Standard
TACAMO−Take Charge and Move Out
TCAM−Threat Condition Alerting Message
THREATCON−Threat Condition
T.O. −Technical Order
TPC−Two-Person Control
UCNI−Unclassified Controlled Nuclear Information
US−United States
USAF−United States Air Force
U.S.C. −United States Code
VNIR−Very Near Infrared
Vol−Volume
WSA−Weapons Storage Area
WS3−Weapons Storage and Security System
WSV−Weapons Storage Vault

USERS FEEDBACK

1. Users in the field are highly encouraged to submit comments on this document by removing this page and sending it to HQ AFSPA. Please fill out the following:

User: _____ Unit: _____

Address: _____ DSN: _____

2. Content.

a. Does the document provide a conceptual framework for the topic?

_____ _____

b. Is the information provided accurate? What needs to be updated?

_____ _____

c. Is this publication consistent with other AF documents?

_____ _____

d. Can this publication be better organized for the best understanding of the material presented?

_____

_____ _____

e. Is the information provided useful? If not, how can it be improved?

_____

_____ _____

3. Writing and appearance.

a. Where does the publication need revision to make the writing clear and concise? What words would you use?

_____

_____ _____

b. Are the charts and figures clear and understandable? How would you revise them?

_____ _____

4. Recommended urgent change(s) (if any)?

_____ _____

5. Other comments: _____

_____ _____

6. Please fold and mail comments to HQ AFSPA/SPS or FAX to DSN 246-0648 or Commercial (505) 846-0648. Additional pages may be attached if desired.

Fold here

HQ AFSPA/SPS

86O1 F AVE SE, BLDG 20203B

KIRTLAND AFB, NM 87117-5664

Fold here